"TESTE DE PRIMALIDADE ATRAVÉS DE SOMAS DE JACOBI"

Este exemplar corresponde a redação final da tese devidamente corrigida e defendida por Maria Camargo Ribeiro e aprovada pela Comissão Julgadora.

Campinas, 8 de agosto de 1990

Prof. Dr. Antonio José Engler

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para obtenção do Título de Mestre em Matemática.

TESTE DE PRIMALIDADE ATRAVÉS DE SOMAS DE JACOBI

MARIA CAMARGO RIBEIRO

Orientador

Prof. Dr. ANTÔNIO JOSÉ ENGLER

Dissertação apresentada no Instituto de Matemática, Estatística e Ciência da Computação da Universidade Estadual de Campinas como requisito parcial para obtenção do título de Mestre em Matemática Pura.

- 1.990 -

Agradeço ao Prof. Dr. Antônio José Engler pela orientação segura, disponibilidade, atenção, estímulo, compreensão e paciência; agradeço também a todos que direta ou indiretamente colaboraram na elaboração deste trabalho.

A quem faz da Ciência um instrumento
para tornar o Homem mais feliz.

ÍNDICE

INTRODUÇÃO

Testes de primalidade são bastante utilizados em Criptografia onde existe grande interesse em se obter números primos de aproximadamente 100 dígitos.

O objetivo desse trabalho é verificar se um número natural ímpar n é primo ou composto por meio de Somas de Jacobi.

O teste de primalidade que será descrito aqui tem melhores chances de ser bem sucedido se n é provavelmente primo. Desse modo, antes de começar a executá-lo, o número n deverá ser submetido a alguns testes mais simples que revelam rapidamente, na maioria dos casos, se n é composto. Um desses testes é baseado no seguinte resultado: n é primo se e somente se $x^{(n-1)/2} \equiv \pm 1 \bmod n$ qualquer que seja $x \in Z$, $(x,n) = 1$. Além disso, é sabido que se n é ímpar e composto, a congruência acima é válida no máximo para a metade dos x (mod n) com $(x,n) = 1$. Assim, se para 100 escolhas ao acaso de x com $x \in \{1 , 2 ,..., n-1\}$ obtivermos $x^{(n-1)/2} \equiv \pm 1 \bmod n$, n é provavelmente primo pois a probabilidade de ser composto e ter acontecido a congruência para os 100 números testados é menor ou igual a $1/2^{100}$. Supondo então que não encontramos x tal que $x^{(n-1)/2} \not\equiv \pm 1 \bmod n$ daremos início à análise de n através das Somas de Jacobi.

Todas as etapas do processo que será descrito tem em vista a aplicação do Teorema (2.11); isso porque se todas as suas hipóteses forem satisfeitas tal teorema afirma que para qualquer r divisor de n existe $i \in \{0 , ..., t-1\}$ (para t conveniente conforme especificado no Teorema (2.11)) tal que

$r \equiv n^i \bmod s$. Assim, tudo o que temos a fazer é tomar i percorrendo $\{0 , 1 , ... , t-1\}$ e calcular $r \equiv n^i \bmod s$; para cada r encontrado verificamos se r divide n. Se os únicos divisores de n forem $r = 1$ e $r = n$ declaramos n primo; caso contrário n é composto tendo r como divisor próprio.

Vemos então que todo o trabalho se resume em encontrar condições para que as hipóteses do Teorema (2.11) sejam satisfeitas. Uma dessas hipóteses exige que t e s verifiquem as seguintes condições: t é "pequeno", $s > n^{1/2}$, $a^t \equiv 1 \bmod s$ para todo $a \in Z$ com $(a,s) = 1$ e a fatoração completa de t e s é conhecida; além disso $(n,s.t) = 1$. Tais s e t são facilmente selecionados se utilizarmos a Proposição (2.8). t deve ser o menor possível visto que quanto menor o t mais rápido percorremos $r \equiv n^i \bmod s$ $i \in \{0 , 1 , ... , t-1\}$; além disso as outras duas condições que analisaremos abaixo tem de ser satisfeitas para qualquer p divisor de t e isso sugere a escolha de t de modo que tenha um número pequeno de divisores.

As outras duas hipóteses adicionais: (2.12) e (2.13) precisam ser examinadas com mais cuidado.

As condições que tornam válida (2.12) serão discutidas no terceiro parágrafo do texto através das Proposições (3.42); (3.43); (3.52); (3.54); (3.56) e (3.60).

Para a validade de (2.13) recorremos ao Teorema (3.21); ele afirma que se temos (3.22) e (2.12) então (2.13) é satisfeita.

Deste modo o Teorema (3.21) se torna um dos resultados mais importantes do texto, pois, a partir de sua validade poderemos utilizar o Teorema (2.11), e, exatamente para obter a condição (3.22) é que necessitamos das Somas de Jacobi. Elas serão estudadas nos parágrafos seguintes.

O §4 se resume no Teorema (4.31) que fornece, a partir de Somas de Jacobi, um critério para que (3,22) seja satisfeita dado p primo ímpar. O Teorema (4.31) também apresenta um critério que indica se n é composto.

No §5 demonstraremos cinco teoremas que esgotam o caso p = 2. Cada um desses teoremas possui uma condição; se tal condição, expressa por uma congruência, for satisfeita teremos a validade de (3.22); se tal condição não ocorre declaramos que n é composto.

Finalmente, o §1 é introdutório; nele fazemos um pequeno estudo dos números inteiros p-ádicos.

§ 1 Breve estudo dos números inteiros p-ádicos

Neste parágrafo introduziremos números inteiros p-ádicos, algumas de suas propriedades e provaremos resultados que são importantes para a melhor compreensão do texto. Não temos por objetivo, entretanto, fazer um estudo detalhado do conjunto dos números p-ádicos; iremos apenas caracterizar os inteiros p-ádicos e utilizar propriedades que são necessárias para o desenvolvimento desse trabalho. Não nos preocuparemos com a análise de completamentos p-ádicos, topologias sobre o conjunto dos números p-ádicos e propriedades das valorizações p-ádicas porque neste contexto estes tôpicos não são importantes.

Das duas caracterizações que conhecemos para números p-ádicos, escolhemos a que é menos usual por ela facilitar algumas demonstrações.

O conjunto dos números inteiros p-ádicos será denotado por Z_p e utilizaremos a caracterização que se segue:

(1.1) Dado $a = (a_i \bmod p^i)_{i=1}^{\infty} \in \prod_{i=1}^{\infty} Z/p^iZ$, a é um inteiro p-ádico se e somente se $a_{i+1} \equiv a_i \bmod p^i$ para todo $i \in Z$, $i \geqslant 1$.

Sabemos que Z/p^iZ é um Anel, logo se definirmos sobre $\prod_{i=1}^{\infty} Z/p^iZ$ as operações de adição e multiplicação coordenada a coordenada, observamos que $\prod_{i=1}^{\infty} Z/p^iZ$ também é um Anel. Z_p é um subconjunto desse produto portanto para verificar se ele é um Anel precisamos apenas das propriedades de fechamento com relação a adição e multiplicação e que qualquer elemento de Z_p possua oposto em Z_p. Claramente Z_p é fechado com relação a adição pois dados $a = (a_i \bmod p^i)_{i=1}^{\infty}$ e $b = (b_i \bmod p^i)_{i=1}^{\infty}$ com $a, b \in Z_p$ temos

$a_{i+1} + b_{i+1} \equiv (a_i + b_i) \bmod p^i$ para todo i e daí $a + b \in Z_p$. Analogamente com relação a multiplicação, $a_{i+1} \cdot b_{i+1} \equiv (a_i . b_i) \bmod p^i$ de modo que $a.b \in Z_p$. Para assegurar que o oposto de um elemento de Z_p pertence a Z_p, seja $a = (a_i \bmod p^i)_{i=1}^{\infty} \in Z_p$; a possui oposto $b = (b_i \bmod p^i)_{i=1}^{\infty}$ em $\prod_{i=1}^{\infty} Z/p^iZ$ logo $a_i + b_i \equiv 0 \bmod p^i$ o que implica em $a_{i+1} + b_{i+1} \equiv 0 \bmod p^i$; combinando essa congruência com $a_i + b_i \equiv 0 \bmod p^i$ obtemos $a_{i+1} + b_{i+1} \equiv a_i + b_i \bmod p^i$; como $a_{i+1} \equiv a_i \bmod p^i$ encontramos $b_{i+1} \equiv b_i \bmod p^i$ o que implica em b pertencer a Z_p. Provamos então que Z_p é um subanel de $\prod_{i=1}^{\infty} Z/p^iZ$.

O anel dos números inteiros Z pode ser visto como um subanel de Z_p identificando-se cada elemento a pertencente a Z com $(a \bmod p^i)_{i=1}^{\infty}$ pertencente a Z_p.

O leitor familiarizado com limites projetivos notará que em (1.1) Z_p foi caracterizado como limite projetivo. Tal afirmação fica mais clara a partir do seguinte lema:

(1.2) LEMA: Dado $a = (a_i \bmod p^i)_{i=1}^{\infty} \in \prod_{i=1}^{\infty} Z/p^iZ$, $a \in Z_p$ se e somente se $a_s \equiv a_r \bmod p^r$ para todo $s \geqslant r$.

PROVA: Dado $s \geqslant r$, $a_s - a_r = a_s - a_{s-1} + a_{s-1} - \ldots\ldots + a_{r+1} - a_r$. A partir de (1.1): $a_{i+1} \equiv a_i \bmod p^i$ obtemos $a_{i+1} - a_i \equiv 0 \bmod p^i$ e claramente $a_{i+1} - a_i \equiv 0 \bmod p^j$ para todo j, $1 \leqslant j \leqslant i$. Em particular a congruência é válida para $j = r$ e $r \leqslant i \leqslant s-1$; obtemos então da igualdade inicial $a_s - a_r \equiv 0 \bmod p^r$, ou equivalentemente, $a_s \equiv a_r \bmod p^r$. Reciprocamente, dado $a_s \equiv a_r \bmod p^r$ para todo $s \geqslant r$, tal congruência é válida para $r = i$ e $s = i+1$; assim temos

$a_{i+1} \equiv a_i \bmod p^i$ para todo i e de acordo com (1.1) a $\in Z_p$. ∎

(1.3) Se compararmos a caracterização de Z_p dada em (1.1) com a que se segue, muitas vezes mais familiar, onde o inteiro p-ádico é representado por $a = \sum_{n=0}^{\infty} x_n.p^n$ com $x_n \in Z$, $0 \leqslant x_n < p$, veremos que as duas caracterizações são equivalentes:

Dado $a = \sum_{n=0}^{\infty} x_n.p^n$ com $x_n \in Z$, $0 \leqslant x_n < p$ para $i \geqslant 1$, chamemos de a_i a soma parcial $\sum_{n=0}^{i-1} x_n.p^n$; temos então $a_{i+1} - a_i = x_i.p^i$ e é fácil observar que $x_i.p^i \equiv 0 \bmod p^i$, portanto $a_{i+1} \equiv a_i \bmod p^i$ de modo que a partir da representação de $a \in Z_p$ como $a = \sum_{n=0}^{\infty} x_n.p^n$ podemos construir um único $a = (a_i \bmod p^i)_{i=1}^{\infty}$, $a \in Z_p$ mas escrito de acordo com a caracterização de (1.1). Reciprocamente dado $a = (a_i \bmod p^i)_{i=1}^{\infty} \in Z_p$, cada $a_i \bmod p^i \in Z/p^iZ$ de modo que se usarmos o Algorítmo Euclideano fazendo sucessivas divisões por p, $a_i \bmod p^i$ pode ser representado de maneira única como $(\sum_{n=0}^{i-1} x_n.p^n) \bmod p^i$ com $x_n \in Z$, $0 \leqslant x_n < p$; isso pode ser feito para todo $i \in Z$, $i \geqslant 1$. Provaremos agora que para qualquer que seja i, os coeficientes dos termos p^n com $0 \leqslant n \leqslant i-1$ são os mesmos. Seja $a_{i+1} \bmod p^{i+1} = (\sum_{n=0}^{i} x_n.p^n) \bmod p^{i+1}$ com $0 \leqslant x_n < p$ e seja $a_i \bmod p^i = (\sum_{n=0} y_n.p^n) \bmod p^i$ com $y_n \in Z$, $0 \leqslant y_n < p$. Sabemos que $a_{i+1} \equiv a_i \bmod p^i$ logo $\sum_{n=0}^{i} x_n.p^n - \sum_{n=0}^{i-1} y_n.p^n \equiv 0 \bmod p^i$ e então $\sum_{n=0}^{i-1} (x_n - y_n).p^n + x_i.p^i \equiv 0 \bmod p^i$, ou equivalentemente, $\sum_{n=0}^{i-1} (x_n - y_n).p^n \equiv 0 \bmod p^i$; observemos no entanto que tanto x_n quanto y_n são não negativos e menores que p, com isso $0 \leqslant | x_n - y_n | \leqslant p-1$; também $\sum_{n=0}^{i-1} p^n$ pode ser vista como a soma dos i primeiros termos de uma progressão geométrica finita de ra-

zão p de modo que $\sum_{n=0}^{i-1} p^n = (p^i - 1)/(p - 1)$; assim $\sum_{n=0}^{i-1}(x_n - y_n).p^n \leqslant (p - 1).\sum_{n=0}^{i-1} p^n \leqslant p^i - 1 < p^i$; analogamente $\sum_{n=0}^{i-1}(y_n - x_n).p^n < p^i$ e então $\sum_{n=0}^{i-1}(x_n - y_n).p^n \equiv 0 \bmod p^i$ se e somente se $\sum_{n=0}^{i-1}(x_n - y_n).p^n = 0$. Como a igualdade vale para todo $i \geqslant 1$ temos $\sum_{n=0}^{i}(x_n - y_n).p^n = 0$, isto é, $\sum_{n=0}^{i-1}(x_n - y_n).p^n = (y_i - x_i).p^i$; contudo $\sum_{n=0}^{i-1}(x_n - y_n).p^n = 0$ logo $(y_i - x_i).p^i = 0$ o que implica em $x_i = y_i$ para todo i; dessa forma $\sum_{n=0}^{i-1}(x_n - y_n).p^n = 0$ se e somente se $x_n = y_n$ para todo n, logo os coeficientes x_n de p^n são os mesmos para todo $a_i \bmod p^i$ e então a pode ser representado de maneira única por $\sum_{n=0}^{\infty} x_n.p^n$.

Uma relação útil entre números inteiros e inteiros p-ádicos é o isomorfismo entre $Z_p/p^m Z_p$ e $Z/p^m Z$; através deste isomorfismo qualquer número inteiro p-ádico quando tomado módulo p^m se identifica com um número inteiro módulo p^m. Para provar esta afirmação seja

$\Psi : \prod_{i=1}^{\infty} Z/p^i Z \longrightarrow Z/p^m Z$ tal que $\Psi((a_i \bmod p^i)_{i=1}^{\infty}) = a_m \bmod p^m$; Ψ é a projeção canônica do produto $\prod_{i=1}^{\infty} Z/p^i Z$ na m-ésima coordenada de modo que é um homomorfismo sobrejetor. Notemos que $\varphi : Z_p \longrightarrow Z/p^m Z$ tal que $\varphi((a_i \bmod p^i)_{i=1}^{\infty}) = a_m \bmod p^m$ é a restrição de Ψ a Z_p, portanto também é um homomorfismo sobrejetor pois para cada $a_m \bmod p^m \in Z/p^m Z$ basta tomarmos $a_i = a_m$ para todo i e obtemos $a = (a_i \bmod p^i)_{i=1}^{\infty}$ em Z_p tal que $\varphi(a) = a_m \bmod p^m$. O Primeiro Teorema do Isomorfismo declara que dado um homomorfismo sobrejetor de grupo $\Psi: G \longrightarrow G'$ temos o grupo quociente $G/Ker\Psi$ isomorfo a G', isto é, $G/Ker\Psi \simeq G'$ onde

Ker Ψ é o núcleo do homomorfismo. Olhando para Z_p e Z/p^mZ como grupos com relação a adição, se obtivermos $p^mZ_p = \{(a_i \bmod p^i)_{i=1}^{\infty} \in Z_p \ / \ a_m \bmod p^m = 0\}$ como núcleo do homomorfismo, teremos a relação desejada. Vamos verificar então se p^mZ_p é o núcleo de φ onde $\mathrm{Ker}\varphi = \{a \in Z_p \ / \ \varphi(a) = 0\}$ com $a = (a_i \bmod p^i)_{i=1}^{\infty}$. Se $a \in \mathrm{Ker}\varphi$, $\varphi(a) = a_m \bmod p^m = 0$ logo $a \in p^mZ_p$ e $\mathrm{Ker}\varphi \subset p^mZ_p$. Reciprocamente se $a \in p^mZ_p$ temos $a_m \bmod p^m = 0$ e assim $\varphi(a) = 0$ de onde $a \in \mathrm{Ker}\varphi$ e portanto $p^mZ_p \subset \mathrm{Ker}\varphi$. Obtemos então $\mathrm{Ker}\varphi = p^mZ_p$ e o homomorfismo está provado.

(1.4) Um outro resultado que será utilizado é a potenciação de Z_p sobre um grupo multiplicativo E, abeliano e finito cuja ordem é uma potência de p. Como E é finito e de ordem potência de p existe $s \in N$ tal que $\zeta^{p^s} = 1$ para todo ζ elemento de E. Quando tomamos $a_m \in Z$ podemos escrevê-lo como $a_m = \sum_{i=0}^{m-1} x_i \cdot p^i + p^m \cdot x$ com $x_i, x \in Z$ e $0 \leqslant x_i < p$ assim se $m \geqslant s$ obtemos $\zeta^{a_m} = \zeta^{\sum_{i=0}^{m-1} x_i \cdot p^i} \cdot (\zeta^{p^s})^{p^{m-s} \cdot x}$ logo para m suficientemente grande ζ^{a_m} não depende de m e será denotado por ζ^a. É fácil observar que esta operação de Z_p sobre E satisfaz as propriedades usuais da potenciação visto que para $a = (a_i \bmod p^i)_{i=1}^{\infty} \in Z_p$, ζ^a corresponde a ζ^{a_m} para algum $a_m \in Z$ e assim temos para todo $\zeta, \eta \in E$, $a, b \in Z_p$:

(1.5) $(\zeta.\eta)^a = \zeta^a.\eta^a$

(1.6) $\zeta^{a+b} = \zeta^a.\zeta^b$

(1.7) $\zeta^{a.b} = (\zeta^a)^b$

(1.8) $\zeta^1 = \zeta$

Seja A um anel; se $1 \in A$ existem em A elementos com inverso multiplicativo; tais elementos são chamados de unidades do Anel e formam o grupo multiplicativo das unidades de A denotado por A^*.

Provaremos a seguir que $Z_p^* = Z_p - pZ_p$ onde $p^m Z_p$ será definido como:

(1.9) $p^m Z_p = \{(a_i \bmod p^i)_{i=1}^{\infty} \in Z_p \ / \ a_m \bmod p^m = 0\}$

Notemos que $a \in pZ_p$ se e somente se $a_1 \equiv 0 \bmod p$, portanto queremos mostrar que se $a = (a_i \bmod p^i)_{i=1}^{\infty} \in Z_p^*$ então $a_1 \not\equiv 0 \bmod p$ pois desejamos obter $a \in Z_p - pZ_p$. Seja $a = (a_i \bmod p^i)_{i=1}^{\infty} \in Z_p \subset \prod_{i=1}^{\infty} Z/p^iZ$; $a \in Z_p^*$ se e somente se cada coordenada $a_i \bmod p^i$ for inversível em Z/p^iZ e isso ocorre se e só se $a_i \bmod p^i \in (Z/p^iZ)^*$ onde $(Z/p^iZ)^* = \{x \in Z/p^iZ \ / \ x \not\equiv 0 \bmod p\}$, logo $a_i \not\equiv 0 \bmod p$ para todo i, em particular $a_1 \not\equiv 0 \bmod p$ de modo que $a \notin pZ_p$, isto é, $a \in Z_p - pZ_p$ e obtemos $Z_p^* \subset Z_p - pZ_p$. Recíprocamente se $a = (a_i \bmod p^i)_{i=1}^{\infty} \in Z_p - pZ_p$ temos $a_1 \not\equiv 0 \bmod p$ mas pelo Lema (1.2) $a_i \equiv a_1 \bmod p$ qualquer $i \geqslant 1$ logo $a_i \not\equiv 0 \bmod p$ para todo $i \geqslant 1$; dessa forma $a_i \bmod p^i \in (Z/p^iZ)^*$ qualquer que seja $i \geqslant 1$; isso faz com que todas as coordenadas sejam inversíveis e assim $Z_p - pZ_p \subset Z_p^*$, portanto

(1.10) $Z_p^* = Z_p - pZ_p$

Observamos então que Z_p é um Anel Local tendo pZ_p como único Ideal Maximal. Essa afirmação pode ser justificada a partir do seguinte Lema:

(1.11) LEMA: Dado um anel A, qualquer que seja $x \in A$, se $x \notin A^*$ então existe um ideal maximal M com $x \in M$.

Aplicando o Lema, se $x \notin Z_p^*$ existe M ideal maximal de Z_p com $x \in M$; no entanto $Z_p^* = Z_p - pZ_p$, portanto $x \in pZ_p$ e então $M \subset pZ_p$; obtemos assim $M = pZ_p$ e pZ_p é o único ideal maximal de Z_p.

Afirmamos que qualquer número inteiro p-ádico diferente de zero pode ser escrito de maneira única como $a = p^m.u$ com $m \in N$ e $u \in Z_p^*$. Tomando $a = (a_i \bmod p^i)_{i=1}^{\infty}$ um inteiro p-ádico genérico, temos duas possibilidades: $a \notin pZ_p$ ou $a \in pZ_p$.

Na primeira possibilidade $a \notin pZ_p$ e a já é uma unidade, podendo ser escrito na forma $p^m.\ u$ com $m = 0$ e $u = a$.

Na segunda possibilidade $a \in pZ_p$ então $a_1 \equiv 0 \bmod p$. Seja m+1 o menor índice tal que $a_{m+1} \not\equiv 0 \bmod p^{m+1}$, logo $a_i \equiv 0 \bmod p^i$ para todo $i \leqslant m$ e de acordo com (1.9) $a \in p^m Z_p$ podendo ser escrito como $a = p^m.u$ para $u = (u_i \bmod p^i)_{i=1}^{\infty} \in Z_p$. Para comprovar que u é uma unidade notemos que $a_{m+1} \equiv p^m.u_{m+1} \bmod p^{m+1}$, mas $a_{m+1} \not\equiv 0 \bmod p^{m+1}$, assim $p^m.u_{m+1} \not\equiv 0 \bmod p^{m+1}$ e portanto $u_{m+1} \not\equiv 0 \bmod p$; utilizando o Lema (1.2) temos $u_{m+1} \equiv u_1 \bmod p$ o que implica em $u_1 \not\equiv 0 \bmod p$, isto é, $u \in Z_p^*$.

Provamos então que qualquer número inteiro p-ádico diferente de zero pode ser escrito como $a = p^m.u$. Para assegurar a unicidade, seja $a = p^m.u = p^m.w$ com $w = (w_i \bmod p^i)_{i=1}^{\infty}$; observemos que $p^m.u_i \equiv p^m.w_i \bmod p^i$ qualquer $i \geqslant 1$, logo $p^m.(u_i - w_i) \equiv 0 \bmod p^i$; para $i > m$ tal congruência ocorre se e somente se $u_i - w_i \equiv 0 \bmod p^{i-m}$ de modo que $u_i \equiv w_i \bmod p^{i-m}$ para

$i > m$; através de Lema (1.2) temos $u_i \equiv u_{i-m} \bmod p^{i-m}$ e $w_i \equiv w_{i-m} \bmod p^{i-m}$, consequentemente $u_{i-m} \equiv w_{i-m} \bmod p^{i-m}$ para todo $i > m$; fazendo $j=i-m$ obtemos $u_j = w_j \bmod p^j$ qualquer $j \geqslant 1$, então $(u_i \bmod p^i)_{i=1}^{\infty} = (w_i \bmod p^i)_{i=1}^{\infty}$, ou equivalentemente, $u = w$ e a representação de a como $p^m.u$ é única.

(1.12) Resulta daí que $p^m\mathbb{Z}_p$ são os únicos ideais de $\mathbb{Z}_p$ e assim $\mathbb{Z}_p$ é um domínio de ideais principais.

(1.13) Valorização p-ádica de $a = p^m.u \in \mathbb{Z}_p$, com $u \in \mathbb{Z}_p^*$ e $a \neq 0$, será definida como o expoente de p. Denotaremos $v_p(a) = m$. Para extendermos a valorização para todo o anel $\mathbb{Z}_p$ definiremos $v_p(0) = \infty$.

Se representarmos o número inteiro p-ádico a como a série $\sum_{n=0}^{\infty} x_n.p^n$ com $x_n \in \mathbb{Z}$, $0 \leqslant x_n < p$, a valorização p-ádica de a corresponderá ao menor expoente m tal que $x_m \neq 0$.

O anel $\mathbb{Z}_p$ é um domínio de integridade e tem como corpo de frações o conjunto dos números p-ádicos denotado por $\mathbb{Q}_p$. Cada elemento de $\mathbb{Q}_p$ pode ser representado como uma série $\sum_{i \geqslant k}^{\infty} x_i.p^i$ com $k \in \mathbb{Z}$ e $0 \leqslant x_i < p$. Observamos então que a valorização p-ádica definida acima pode ser extendida ao corpo $\mathbb{Q}_p$.

Dando sequência, provaremos a propriedade mais importante a respeito de números inteiros p-ádicos presente neste texto:

(1.14) $a^{\mathbb{Z}_p} = 1 + p^m\mathbb{Z}_p$ para $m = v_p(a-1)$ se $m \geqslant 1$ e $p \neq 2$ e $m \geqslant 2$ quando $p=2$

Antes de esclarecer o significado de a^{Z_p} e demonstrar a igualdade precisamos de alguns resultados auxiliares.

Para todo $m \in N$, $m \geqslant 1$ provaremos o seguinte:

(1.15) $1 + p^m Z_p = \{a = (a_i \bmod p^i)_{i=1}^{\infty} \in Z_p \ / \ a_m \equiv 1 \bmod p^m\}$ é um subgrupo do grupo multiplicativo Z_p^*.

Primeiramente notemos que $1 + p^m Z_p \subset Z_p^*$ pois $Z_p^* = Z_p - pZ_p$ e claramente se $a_m \equiv 1 \bmod p^m$ então $a_1 \not\equiv 0 \bmod p$ e $a \notin pZ_p$. Para verificar que $1 + p^m Z_p$ é fechado com relação a multiplicação, dados $a = (a_i \bmod p^i)_{i=1}^{\infty}$ e $b = (b_i \bmod p^i)_{i=1}^{\infty}$, se $a,b \in 1 + p^m Z_p$ temos $a_m . b_m \equiv 1 \bmod p^m$ portanto $a.b \in 1 + p^m Z_p$. Observemos agora que se $a \in 1 + p^m Z_p$, a possui inverso $c = (c_i \bmod p^i)_{i=1}^{\infty}$ em Z_p^* com $a_i . c_i \equiv 1 \bmod p^i$ para todo $i \geqslant 1$, em particular $a_m . c_m \equiv 1 \bmod p^m$, mas $a_m \equiv 1 \bmod p^m$ o que implica em $c_m \equiv 1 \bmod p^m$ e portanto $c \in 1 + p^m Z_p$. Com isso provamos que $1 + p^m Z_p$ é um grupo multiplicativo pois a propriedade associativa é verificada e $1 \in 1 + p^m Z_p$.

Nessa próxima etapa demonstraremos que

(1.16) $1 + p^m Z_p$ é um Z_p-módulo

Para isso precisamos definir a^x com $a \in 1 + p^m Z_p$ e $x \in Z_p$.

Para $i \geqslant 1$, seja

(1.17) $K_i = \{a_i \bmod p^i \in Z/p^i Z / \ a_1 \equiv 1 \bmod p\}$

É fácil observar que K_i é um subgrupo do grupo multipli-

cativo $(\mathbb{Z}/p^i\mathbb{Z})^*$ e K_i tem ordem p^{i-1}. Dado $a = (a_i \bmod p^i)_{i=1}^{\infty} \in \mathbb{Z}_p$, se $a_i \bmod p^i \in K_i$ e $x = (x_i \bmod p^i)_{i=1}^{\infty} \in \mathbb{Z}_p$ com $x_i \in \mathbb{Z}$, conhecemos $(a_i \bmod p^i)^x$. Dado $a = (a_i \bmod p^i)_{i=1}^{\infty} \in 1 + p^m\mathbb{Z}_p$ temos $a_i \bmod p^i \in K_i$ para todo $i \geqslant 1$; definimos então $a^x = ((a_i \bmod p^i)^x)_{i=1}^{\infty}$ com $a^x \in \prod_{i=1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}$.

Seja $\varphi : \mathbb{Z}_p \times (1 + p^m\mathbb{Z}_p) \longrightarrow 1 + p^m\mathbb{Z}_p$ tal que $\varphi(x,a) = a^x$.

Para provar que $1 + p^m\mathbb{Z}_p$ é um $\mathbb{Z}_p$-módulo devemos verificar que φ é uma função e satisfaz as propriedades de $\mathbb{Z}_p$-módulo.

Seja $b = (b_i \bmod p^i)_{i=1}^{\infty} \in \prod_{i=1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}$, $b_i \in \mathbb{Z}$, tal que $b = a^x$, ou seja, $b_i \bmod p^i = (a_i \bmod p^i)^x$ para todo $i \geqslant 1$. Provar que $a^x = b \in \mathbb{Z}_p^*$ é equivalente a demonstrar que $b_{i+1} \equiv b_i \bmod p^i$ para todo $i \geqslant 1$. Recordemos que $(a_{i+1} \bmod p^{i+1})^x = (a_{i+1} \bmod p^{i+1})^{x_j} = (a_{i+1})^{x_j} \bmod p^{i+1}$ para j suficientemente grande, logo $b_{i+1} \equiv (a_{i+1})^{x_j} \bmod p^{i+1}$ e então (1.18) $b_{i+1} \equiv (a_{i+1})^{x_j} \bmod p^i$; observemos no entanto que j pode ser escolhido de modo que $(a_i)^{x_j} \bmod p^i = (a_i \bmod p^i)^{x_j}$ e $(a_i \bmod p^i)^{x_j} = (a_i \bmod p^i)^x = b_i \bmod p^i$; por outro lado $a \in 1 + p^m\mathbb{Z}_p \subset \mathbb{Z}_p^*$ e daí $a_{i+1} \equiv a_i \bmod p^i$ para todo $i \geqslant 1$, consequentemente $(a_{i+1})^{x_j} \equiv (a_i)^{x_j} \bmod p^i$ para todo $x_j \in \mathbb{Z}$, mas $(a_i)^{x_j} \bmod p^i = b_i \bmod p^i$, assim $(a_{i+1})^{x_j} \equiv b_i \bmod p^i$ e substituindo esse valor em (1.18) encontramos $b_{i+1} \equiv b_i \bmod p^i$ e desse modo $a^x \in \mathbb{Z}_p^*$.

Para provar que $a^x \in 1 + p^m\mathbb{Z}_p$, notemos que $a_m \equiv 1 \bmod p^m$ assim $a_m \bmod p^m = 1$, mas $(a_m \bmod p^m)^x = (a_m \bmod p^m)^{x_j}$ para algum

$x_j \in N$, com isso $(a_m \bmod p^m)^x = 1^{x_j} = 1$ e . portanto $a^x = ((a_i \bmod p^i)^x)_{i=1}^{\infty} \in 1 + p^m Z_p$.

Passaremos agora a verificar as propriedades que fazem de $1 + p^m Z_p$ um Z_p-módulo. Por (1.15) $1 + p^m Z_p$ é um grupo multiplicativo, assim, dados $a = (a_i \bmod p^i)_{i=1}^{\infty}$, $b = (b_i \bmod p^i)_{i=1}^{\infty}$ com $a,b \in 1 + p^m Z_p$; $x = (x_i \bmod p^i)_{i=1}^{\infty}$, $y = (y_i \bmod p^i)_{i=1}^{\infty} \in Z_p$ com a_i, b_i, x_i, $y_i \in Z$ temos:

M1) $(a.b)^x = ((a_i.b_i \bmod p^i)^x)_{i=1}$, para cada $i \geq 1$ existe $j \in Z$ suficientemente grande tal que $(a_i.b_i \bmod p^i)^x = (a_i.b_i \bmod p^i)^{x_j} = (a_i \bmod p^i)^{x_j}.(b_i \bmod p^i)^{x_j} = (a_i \bmod p^i)^x.(b_i \bmod p^i)^x$, assim $((a_i.b_i \bmod p^i)^x)_{i=1}^{\infty} = ((a_i \bmod p^i)^x.(b_i \bmod p^i)^x)_{i=1}^{\infty} = ((a_i \bmod p^i)^x)_{i=1}^{\infty}.((b_i \bmod p^i)^x)_{i=1}^{\infty}$, portanto $(a.b)^x = a^x.b^x$.

M2) $a^{x+y} = ((a_i \bmod p^i)^{x+y})_{i=1}^{\infty}$; desde que $x + y = ((x_i + y_i) \bmod p^i)_{i=1}^{\infty} \in Z_p$, para cada $i \geq 1$ existe j suficientemente grande tal que $(a_i \bmod p^i)^{x+y} = (a_i \bmod p^i)^{x_j + y_j} = (a_i \bmod p^i)^{x_j}.(a_i \bmod p^i)^{y_j} = (a_i \bmod p^i)^x.(a_i \bmod p^i)^y$, assim $((a_i \bmod p^i)^x.(a_i \bmod p^i)^y)_{i=1}^{\infty} = a^x.a^y$ e portanto $a^{x+y} = a^x.a^y$.

M3) Para calcular $a^{x.y}$, notemos que $x.y = (x_i.y_i \bmod p^i)_{i=1}^{\infty}$, então podemos obter j grande o suficiente satisfazendo simultaneamente as igualdades: $(a_i \bmod p^i)^{x.y} = (a_i \bmod p^i)^{x_j.y_j}$, $(a_i \bmod p^i)^{x_j} = (a_i \bmod p^i)^x$ e $((a_i \bmod p^i)^x)^{y_j} = ((a_i \bmod p^i)^x)^y$ para todo $i \geq 1$ logo $a^{x.y} = ((a_i \bmod p^i)^{x.y})_{i=1} = (((a_i \bmod p^i)^x)^y)_{i=1}$ e portanto $a^{x.y} = (a^x)^y$.

M4) $a^1 = ((a_i \bmod p^i)^1)_{i=1}^{\infty} = (a_i \bmod p^i)_{i=1}^{\infty}$ e portanto $a^1 = a$.

Com isso provamos que $1 + p^m Z_p$ é um Z_p-módulo, mais ainda

é um Z_p-módulo livre de Z_p-torção.

Dado $a \in 1 + p^m Z_p$ seja $a^{Z_p} = \{a^x \ / \ x \in Z_p\}$. Já demonstramos que $a^x \in 1 + p^m Z_p$ para todo $x \in Z_p$, portanto

(1.19) $\quad a^{Z_p} \subset 1 + p^m Z_p$

Mostraremos a seguir que $1 + p^m Z_p \subset a^{Z_p}$. Essa prova pode ser feita de um modo mais abstrato e talvez até mais elegante utilizando-se limite projetivo; no entanto optamos aqui por um caminho diferente no qual é necessário apenas o conhecimento de propriedades elementares de grupos. Essa escolha evita ao leitor o contato com limites projetivos que não mais seriam encontrados em todo o texto. De modo geral nesse trabalho o caminho escolhido para as demonstrações é o mais elementar possível, mesmo que em algumas situações torne as provas um pouco mais longas.

A demonstração que faremos agora é construtiva e consiste em exibir para cada $b \in 1 + p^m Z_p$ um elemento $x \in Z_p$ tal que $b = a^x$. Desse modo $b \in a^{Z_p}$ qualquer que seja $b \in 1 + p^m Z_p$ e chegamos na relação desejada. (Lembremos que $v_p(a-1) = m$)

Faremos a seguir as afirmações A1), A2) e A3) que só serão justificadas após concluirmos que $1 + p^m Z_p \subset a^{Z_p}$.

Seja

(1.20) $\quad K_i = \{x_i \bmod p^i \in Z/p^i Z \ / \ x_i \equiv 1 \bmod p\}$

Dado $a = (a_i \bmod p^i)_{i=1}^{\infty} \in Z_p$ com $v_p(a-1) = m$, $a_i \in Z$,

$m \geqslant 1$ para p primo, $p \neq 2$ e $m \geqslant 2$ para $p=2$, afirmamos:

A1) A ordem de $a_i \bmod p^i$ em K_i, denotada por $o(a_i \bmod p^i)$, é igual a 1 se $i \leqslant m$ e igual a p^{i-m} se $i > m$. Denotaremos por $\langle a_i \bmod p^i \rangle$ o subgrupo de K_i gerado por $a_i \bmod p^i$.

A2) K_i é um grupo multiplicativo cíclico de ordem p^{i-1} e qualquer elemento da forma $(1 + p.u) \bmod p^i$ com $u \in Z - pZ$ é gerador de K_i.

A3) Se $b \in 1 + p^m Z_p$, $b = (b_i \bmod p^i)_{i=1}^{\infty}$ então $b_i \bmod p^i \in \langle a_i \bmod p^i \rangle$, isto é, existe $s_i \in N$, $0 \leqslant s_i < p^{i-m}$ tal que $b_i \bmod p^i = (a_i \bmod p^i)^{s_i}$.

Vamos agora exibir $x \in Z_p$ tal que $b = a^x$. Por A3) temos $b_i \bmod p^i \in \langle a_i \bmod p^i \rangle$, assim $i \leqslant m$ implica em $b_i \bmod p^i = a_i \bmod p^i$ visto que nesse caso $o(a_i \bmod p^i) = 1$; se $i > m$ existe $s_{i+1} \in N$ tal que $b_{i+1} \bmod p^{i+1} = (a_{i+1} \bmod p^{i+1})^{s_{i+1}}$, isto é, $b_{i+1} \equiv (a_{i+1})^{s_{i+1}} \bmod p^{i+1}$, logo $b_{i+1} \equiv (a_{i+1})^{s_{i+1}} \bmod p^i$, mas $b \in Z_p$ de modo que $b_{i+1} \equiv b_i \bmod p^i$ e então $b_i \equiv (a_{i+1})^{s_{i+1}} \bmod p^i$; no entanto $a_{i+1} \equiv a_i \bmod p^i$ o que implica em $b_i \equiv (a_i)^{s_{i+1}} \bmod p^i$. Por outro lado A3) nos assegura a existência de $s_i \in N$ tal que $b_i \bmod p^i = (a_i \bmod p^i)^{s_i}$, isto é, $b_i \equiv (a_i)^{s_i} \bmod p^i$. Combinando as duas últimas congruências encontramos $(a_i)^{s_{i+1}} \equiv (a_i)^{s_i} \bmod p^i$. Como $a \in 1 + p^m Z_p$ (pois $v_p(a-1)=m$), $a_i \bmod p^i$ possui inverso em Z/p^iZ, logo $(a_i)^{s_{i+1}-s_i} \equiv 1 \bmod p^i$, mas por A1) $o(a_i \bmod p^i) = p^{i-m}$ então p^{i-m} é divisor de $s_{i+1} - s_i$ (essa relação será representada por $p^{i-m}/(s_{i+1} - s_i)$), portanto $s_{i+1} = s_i + k.p^{i-m}$ para algum $k \in Z$. Notamos então que

$(a_i \bmod p^i)^{s_{i+1}} = (a_i \bmod p^i)^{s_i} . (a_i \bmod p^i)^{p^{i-m}.k}$ mas $((a_i \bmod p^i)^{p^{i-m}})^k = 1$ o que implica em $(a_i \bmod p^i)^{s_{i+1}} = (a_i \bmod p^i)^{s_i}$. Da relação $s_{i+1} \equiv s_i \bmod p^{i-m}$ obtemos $s_{i+m+1} \equiv s_{i+m} \bmod p^i$. Seja $x_i = s_{i+m}$; claramente $x_{i+1} \equiv x_i \bmod p^i$; temos então $(a_i \bmod p^i)^{x_i} = (a_i \bmod p^i)^{s_{i+m}} = (a_i \bmod p^i)^{s_i}$, mas por hipótese $b_i \bmod p^i = (a_i \bmod p^i)^{s_i}$ portanto $b_i \bmod p^i = (a_i \bmod p^i)^{x_i}$ para todo $i \in N$, $i \geqslant 1$. Como $x_{i+1} \equiv x_i \bmod p^i$, fazendo $x = (x_i \bmod p^i)_{i=1}^{\infty}$ concluimos que $x \in Z_p$. Observemos no entanto que $a^x = ((a_i \bmod p^i)^x)_{i=1}^{\infty}$ com $(a_i \bmod p^i)^x = (a_i \bmod p^i)^{x_j}$ para j suficientemente grande, mas $x_j \equiv x_i \bmod p^i$ para $j \geqslant i$ e $o(a_i \bmod p^i) = p^{i-m}$ se $i > m$ e $o(a_i \bmod p^i) = 1$ se $i \leqslant m$, portanto $(a_i \bmod p^i)^{x_j} = (a_i \bmod p^i)^{x_i}$ de modo que $(a_i \bmod p^i)^x = (a_i \bmod p^i)^{x_i}$ para todo $i \geqslant 1$. Obtemos então $b = (b_i \bmod p^i)_{i=1}^{\infty} = ((a_i \bmod p^i)^{x_i})_{i=1}^{\infty} = ((a_i \bmod p^i)^x)_{i=1}^{\infty}$ e chegamos a $b = a^x$.

Assim qualquer que seja $b \in 1 + p^m Z_p$ podemos encontrar $x \in Z_p$ tal que $a^x = b$, consequentemente $b \in a^{Z_p}$ e então $1 + p^m Z_p \subset a^{Z_p}$. Combinando essa inclusão com (1.19): $a^{Z_p} \subset 1 + p^m Z_p$ obtemos a igualdade (1.14): $a^{Z_p} = 1 + p^m Z_p$.

Provaremos a seguir as afirmações A1), A2) e A3).

A1) Para calcular a ordem de $a_i \bmod p^i$ em $K_i \subset (Z/p^i Z)^*$ (K_i definido em (1.20)) recordemos que por hipótese $v_p(a-1) = m$ (v_p definida em (1.13)), assim $a-1 = p^m.u$ onde $u = (u_i \bmod p^i)_{i=1}^{\infty} \in Z_p^*$, e temos então $a_m \equiv 1 \bmod p^m$ o que implica em $a_m \equiv 1 \bmod p^i$ para todo $i \leqslant m$; no entanto utilizando o

Lema (1.2), $a_m \equiv a_i \bmod p^i$ para todo $i \leqslant m$ e combinando essa congruência com a anterior obtemos $a_i \equiv 1 \bmod p^i$ para todo $i \leqslant m$, portanto $o(a_i \bmod p^i) = 1$ para $i \leqslant m$.

Para $i > m$ temos $a_i \bmod p^i = (1 + p^m.u_i) \bmod p^i$ de modo que dado $r \in N$, $a_i^{p^r} \equiv (1 + p^m.u_i)^{p^r} \bmod p^i$, ou equivalentemente, $a_i^{p^r} \equiv (1 + p^{m+r}.u_i + \sum_{j=2}^{p^r} \binom{p^r}{j}.(p^m.u_i)^j) \bmod p^i$. Se provarmos que:

(1.21) $p^{m+r+1} \nmid \sum_{j=2}^{p^r} \binom{p^r}{j}.(p^m.u_i)^j$ para $r \in N^*$

teremos $\sum_{j=2}^{p^r} \binom{p^r}{j}.(p^m.u_i)^j = p^{m+r+1}.t_i$ para algum $t_i \in Z$, consequentemente $a_i^{p^r} \equiv (1 + p^{m+r}.(u_i + p.t_i)) \bmod p^i$. A ordem de $a_i \bmod p^i$ será o menor expoente p^r tal que $a_i^{p^r} \equiv 1 \bmod p^i$, assim devemos obter o menor r tal que $1 + p^{m+r}.(u_i + p.t_i) \equiv 1 \bmod p^i$, isto é, $p^{m+r}.(u_i + p.t_i) \equiv 0 \bmod p^i$; observemos no entanto que $u \in Z_p^*$, logo $(u_i + p.t_i) \not\equiv 0 \bmod p$ e então a última congruência ocorre se e somente se $p^{m+r} \equiv 0 \bmod p^i$, mas essa congruência acontece se e somente se p^i / p^{m+r}. Claramente o menor r que satisfaz p^i / p^{m+r} é $r = i-m$, portanto se (1.21) é válida temos $o(a_i \bmod p^i) = p^{i-m}$.

Resta-nos então provar que (1.21) é verdadeira. Para isso analisaremos os termos da somatória $\sum_{j=2}^{p^r} \binom{p^r}{j}.(p^m.u_i)^j$ inicialmente para $2 \leqslant j < p^r$ e em seguida discutiremos o caso $j = p^r$. Dado j, $2 \leqslant j < p^r$ temos $\binom{p^r}{j} = \frac{p^r.(p^r - 1).(p^r - 2).....(p^r - (j - 1))}{1.2.....(j - 1).j}$.

Seja $W = \{w \in N / 1 \leqslant w \leqslant j-1\}$. Notemos que se p^t / w e $p^{t+1} \nmid w$ com $t \in N$, $t \geqslant 1$, então $p^t / (p^r - w)$ pois $r > t$. Se $w \in W$, temos $p^r - 1 \leqslant p^r - w \leqslant p^r - (j - 1)$; consequentemente, para cada $w \in W$ no denominador de $\binom{p^r}{j}$ com p^t / w e $p^{t+1} \nmid w$ existe $p^r - w$ no numerador

tal que p^t / w, isto é, $(p^r - w)/ w = x/ y$ com $(y,p) = 1$. Sabemos no entanto que $\binom{p^r}{j} \in N$ e pelo fato dos fatores p dos termos $w \in W$ terem sido "cancelados" no denominador, concluimos que $p^{r-d} / \binom{p^r}{j}$ dado $d = v_p(j)$, ou seja, $(j,p^r) = p^d$. Claramente se $(j,p) = 1$ temos $d=0$ e então $p^r / \binom{p^r}{j}$. Assim, se $d=0$, para $2 \leqslant j < p^r$ temos $m.j \geqslant m + 1$; com isso $p^{m+1} / (p^m.u_i)^j$ e portanto $p^{r+m+1} / \binom{p^r}{j}.(p^m.u_i)^j$. Se $d \neq 0$ façamos $j = p^d.f$ com $f \in N$. Notemos que $2^d = (1+1)^d = \sum_{i=0}^{d} \binom{d}{i}$; a somatória possui d+1 elementos e cada $\binom{d}{i}$ é um número natural diferente de zero de modo que $2^d \geqslant d+1$. Dado $p \neq 2$ e $m \geqslant 1$ temos $m.j = m.p^d.f \geqslant m.p^d > m.2^d \geqslant m.(d+1)$ logo $m.j > m.d + m$ e então $m.j \geqslant d + m + 1$, com isso $p^{m+d+1} / (p^m.u_i)^j$; como $p^{r-d} / \binom{p^r}{j}$ obtemos

(1.22) $p^{m+r+1} / \binom{p^r}{j}.(p^m.u_i)^j$ para $2 \leqslant j < p^r$, $p \neq 2$ e $m \geqslant 1$

Dado $p = 2$ temos $m.j = m.p^d.f \geqslant m.p^d \geqslant m.(d+1)$. Se $m \geqslant 2$ temos $m.d + m \geqslant d + 1 + m$, ou seja, $m.j \geqslant m + d + 1$ e então $p^{m+d+1} / (p^m.u_i)^j$; como $p^{r-d} / \binom{p^r}{j}$ obtemos

(1.23) $p^{r+m+1} / \binom{p^r}{j}.(p^m.u_i)^j$ para $2 \leqslant j < p^r$, $p = 2$ e $m \geqslant 2$

No entanto, se $m = 1$ e $p = 2$ não podemos afirmar que $m.p^d \geqslant m + d + 1$; basta tomarmos $m = d = 1$ e encontraremos $2 < 3$.

Dado $j = p^r$ temos $\binom{p^r}{j}.(p^m.u_i)^j = (p^m.u_i)^{p^r}$. Para $p \neq 2$, $p^r > 2^r \geqslant r + 1$, ou seja, $p^r > r + 1$, logo $p^r \geqslant r + 2$ e consequentemente $m.p^r \geqslant m.(r + 2)$; como $m \geqslant 1$ e $r \geqslant 1$ obtemos $m.r + 2.m \geqslant r + m + 1$ portanto $m.p^r \geqslant r + m + 1$. Concluímos então que

(1.24) $p^{r+m+1} / (p^m.u_i)^{p^r}$ se $p \neq 2$

Dado $p = 2$, $p^r \geqslant r + 1$ logo $m.p^r \geqslant m.(r + 1)$. Se $m \geqslant 2$

então $m.(r+1) = m.r + m \geqslant 2.r + m \geqslant r + 1 + m$, portanto

(1.25) $p^{m+r+1} / (p^m.u_i)^{p^r}$ se $p = 2$ e $m \geqslant 2$

Concluindo, se p é um número primo diferente de 2 as relações (1.22) e (1.24) nos asseguram que $p^{m+r+1} / \binom{p^r}{j}.(p^m.u_i)^j$ para todo $m \geqslant 1$ e $2 \leqslant j \leqslant p^r$ de modo que $p^{m+r+1} / \sum_{j=2}^{p^r} \binom{p^r}{j}.(p^m.u_i)^j$ e (1.21) é verificada. Se $p = 2$ as relações (1.23) e (1.25) nos asseguram que $p^{m+r+1} / \sum_{j=2}^{p^r} \binom{p^r}{j}.(p^m.u_i)^j$ desde que $m \geqslant 2$ e então (1.21) é verdadeira para $m \geqslant 2$.

Cabe aqui salientar que a igualdade (1.14): $a^{Z_p} = 1 + p^m Z_p$ só é válida para $p = 2$ quando $m \geqslant 2$, visto que para $m = 1$ a afirmação A1) não é verdadeira (basta tomarmos 3 mod 8; $v_2(3 - 1) = m$ e $m = 1$, $i = 3$ e $o(3 \bmod 8) = 2 \neq 2^{i-m}$) e A1) é fundamental para a prova de (1.14).

A2) Claramente K_i possui p^{i-1} elementos; a partir de A1) para todo $u \in Z$, com $(u,p) = 1$, o elemento $(1 + p.u) \bmod p^i \in K_i$ pois $v_p(p.u) = 1$, logo $\langle (1 + p.u) \bmod p^i \rangle$ gera um subgrupo cíclico de K_i com o mesmo número de elementos de K_i, portanto $K_i = \langle (1 + p.u) \bmod p^i \rangle$, consequentemente K_i é um grupo multiplicativo cíclico.

A3) Seja $b = (b_i \bmod p^i)_{i=1}^{\infty} \in 1 + p^m Z_p$ o que implica em $v_p(b - 1) = v \geqslant m$. Vemos que $(b_i \bmod p^i) \in K_i$ e por A1) $o(b_i \bmod p^i) = 1$ se $i \leqslant v$ e $o(b_i \bmod p^i) = p^{i-v}$ se $i > v$; em qualquer caso $o(b_i \bmod p^i) / p^{i-m}$ visto que $v \geqslant m$; no entanto provamos em A2) que K_i é um grupo multiplicativo cíclico e os subgrupos de

um grupo cíclico são ordenados por inclusão de modo que se $o(b_i \bmod p^i) / p^{i-m}$ e $o(a_i \bmod p^i) = p^{i-m}$ então $b_i \bmod p^i \in \langle a_i \bmod p^i \rangle$ e com isso existe $s_i \in N$ tal que $b_i \bmod p^i = (a_i \bmod p^i)^{s_i}$.

Dando prosseguimento provaremos os últimos resultados desse parâgrafo e com eles encerraremos o estudo de números p-ádicos. Exibiremos a seguir isomorfismos de grupos relacionados a Z_2^* e Z_p^* para $p \neq 2$. São eles:

(1.26) $Z_p^* \simeq Z/(p-1)Z \times (1 + pZ_p)$ se $p \geqslant 3$

(1.27) $Z_2^* \simeq 1 + 2Z_2 \simeq \{\pm 1\} \times (1 + 4Z_2)$

Para demonstrar esses isomorfismos alguns resultados serão necessários:

(1.28) Dados os conjuntos A , B , C e os homomorfismos de grupos $f : A \longrightarrow B$ e $g : B \longrightarrow C$, a sequência $A \xrightarrow{f} B \xrightarrow{g} C$ é chamada sequência exata se f é injetiva, g é sobrejetiva e o conjunto imagem do homomorfismo f é igual ao núcleo do homomorfismo g (isto é, Im f = Ker g).

(1.29) LEMA: Seja B um grupo e $p : B \longrightarrow B$ homomorfismo de grupos multiplicativos tal que $p^2 = p \circ p = p$. Então:

(a) $\text{Im } p = \{x \in B \ / \ p(x) = x\}$

(b) $\text{Ker } p \cap \text{Im } p = \{1\}$

(c) $B = \text{Ker } p \otimes \text{Im } p$

PROVA: (a) Se $x \in \text{Im } p$ então existe $y \in B$ tal que $p(y) = x$ logo $p(x) = p \circ p(y) = p^2(y) = p(y) = x$, assim se $x \in \text{Im } p$, $p(x) = x$, portanto $\text{Im } p \subset \{x \in B \ / \ p(x) = x\}$. Por outro lado se $x \in \{x \in B \ / \ p(x) = x\}$ é fácil observar que $x \in \text{Im } p$; com isso $\{x \in B \ / \ p(x) = x\} \subset \text{Im } p$ e combinando essa inclusão com a inclusão anterior obtemos $\text{Im } p = \{x \in B \ / \ p(x) = x\}$.

(b) Se $x \in \text{Im } p$, por (a) temos $p(x) = x$; se $x \in \text{Ker } p$ então $p(x) = 1$, logo se $x \in \text{Ker } p \cap \text{Im } p$ temos $p(x) = x = 1$, portanto $\text{Im } p \cap \text{Ker } p = \{1\}$.

(c) $\text{Ker } p \times \text{Im } p = \{x.y \ / \ x \in \text{Ker } p \ , \ y \in \text{Im } p\}$. Desde que B é um grupo multiplicativo e $p : B \longrightarrow B$ é homomorfismo de grupos, dado $z \in B$, $p(z) \in B$ possui inverso $p(z)^{-1}$ em B, assim qualquer que seja $z \in B$, $z = z.1 = z.(p(z)^{-1}.p(z)) = (z.p(z)^{-1}).p(z)$. Notemos agora que $p(z) = p((z.p(z)^{-1}).p(z)) = p(z.p(z)^{-1}).p^2(z)$, mas $p^2(z) = p(z)$ logo $p(z) = p(z.p(z)^{-1}).p(z)$ consequentemente $p(z.p(z)^{-1}) = 1$ e então $z.p(z)^{-1} \in \text{Ker } p$; desse modo $z = (z.p(z)^{-1}).p(z)$ com $z.p(z)^{-1} \in \text{Ker } p$ e $p(z) \in \text{Im } p$, portanto $z \in \text{Ker } p \times \text{Im } p$ e com isso $B \subset \text{Ker } p \times \text{Im } p$. Por outro lado, desde que $\text{Im } p \subset B$ e B é um grupo multiplicativo, para todo $x.y \in \text{Ker } p \times \text{Im } p$ temos $x.y \in B$, assim $B = \text{Ker } p \times \text{Im } p$. Para que essa soma seja uma soma direta é necessário que $\text{Ker } p \cap \text{Im } p = \{1\}$, mas essa igualdade já foi verificada em (a), portanto $B \cong \text{Im } p \otimes \text{Ker } p$. ∎

(1.30) PROPOSIÇÃO: Dada a sequência exata de grupos abelianos $1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1$ se existe $h : C \longrightarrow B$, h homomorfismo

de grupos tal que $g \circ h = id_C$ onde id_C é a função identidade então $B \cong A \otimes C$.

PROVA: Seja $p : B \longrightarrow B$ com $p = h \circ g$; $p^2 = p \circ p = (h \circ g) \circ (h \circ g) =$ $= h \circ (g \circ h) \circ g$ mas por hipótese $g \circ h = id_C$ de modo que $p \circ p = h \circ g = p$. Com isso p satisfaz a propriedade (c) do Lema (1.29), logo $B = \text{Ker } p \otimes \text{Im } p$. Como $g \circ h = id_C$, claramente h é um homomorfismo injetivo pois se $h(x) = h(z)$ então $x = g \circ h(x) = g \circ h(z) = z$, assim $g(x) = 1$ se e somente se $h \circ g(x) = 1 = p(x)$ e então $\text{Ker } p = \text{Ker } g$. Pelo fato de f ser injetiva temos $\text{Im } f \cong A$; pela definição de sequência exata $\text{Im } f = \text{Ker } g = \text{Ker } p$, portanto $\text{Ker } p \cong A$. Por outro lado se $x \in \text{Im } p$ então $p(x) = x = h \circ (g(x))$, logo $x \in \text{Im } h$ e se $x \in \text{Im } h$ então existe $y \in C$ tal que $h(y) = x$ logo $p(x) = p \circ h(y) =$ $= (h \circ g) \circ h(y) = h \circ (g \circ h(y))$ mas $g \circ h = id_C$, assim $h \circ (g \circ h(y)) = h(y)$ de modo que $p(x) = h(y) = x$, então $x \in \text{Im } p$, portanto $\text{Im } p = \text{Im } h$. Como h é injetiva temos $\text{Im } h \cong C$, logo $\text{Im } p \cong C$ e portanto $B = \text{Ker } p \otimes \text{Im } p \cong A \otimes C$. ∎

(1.31) LEMA DE NEWTON: Dado K um corpo completo com respeito a valorização não arquimediana $| \ |$ e V o anel de valorização associado, seja f(x) um polinômio com coeficientes em V. Suponhamos que f(x) tem coeficiente líder igual a 1. Se existe um $a_1 \in K$ tal que $|f(a_1)| < 1$ e $|f'(a_1)| = 1$ (f' é a derivada usual), então a sequência $a_2 = a_1 - f(a_1)/f'(a_1)$, $a_3 = a_2 - f(a_2)/f'(a_2)$ ..... converge para uma raiz $a \in V$ de f(x).

PROVA: Introduction to p-Adic Numbers and Valuation Theory -

Geoge Bachman - Theorem 4.1

Para verificar (1.26), seja $i : 1 + pZ_p \longrightarrow Z_p^*$ a função identidade e $\Pi: Z_p^* \longrightarrow (Z/pZ)^*$ a projeção de Z_p^* em sua primeira coordenada, ou seja, dado $a = (a_i \bmod p^i)_{i=1}^{\infty} \in Z_p^*$, $\Pi(a) = a_1 \bmod p$. Provaremos que a sequência $1 \longrightarrow 1 + pZ_p \xrightarrow{i} Z_p^* \xrightarrow{\Pi} (Z/pZ)^* \longrightarrow 1$ é uma sequência exata que satisfaz as condições da Proposição (1.30). Claramente i é um homomorfismo injetivo e Π é um homomorfismo sobrejetivo. Para verificar que $\operatorname{Ker}\Pi = \operatorname{Im} i$ notemos que $\operatorname{Ker}\Pi = \{a = (a_i \bmod p^i)_{i=1}^{\infty} \in Z_p^* / a_1 \equiv 1 \bmod p\}$ e isso ocorre se e somente se $a \in 1 + pZ_p = \operatorname{Im} i$, portanto $\operatorname{Ker}\Pi = \operatorname{Im} i$. Vemos então que a sequência é exata. Para que a sequência exata satisfaça as condições da Proposição (1.30) devemos exibir um homomorfismo $h : (Z/pZ)^* \longrightarrow Z_p^*$ tal que $\Pi \circ h = id$ (onde id é a função identidade). Utilizando o Lema de Newton verificamos que o polinômio $P(D) = D^{p-1} - 1$ pode ser fatorado completamente em Z_p^*; como $(\zeta_{p-1})^j$ é raiz de P(D) para todo $j \in Z$, então $(\zeta_{p-1})^j \in Z_p^*$. Seja $\zeta_{p-1} = (x_i \bmod p^i)_{i=1}^{\infty}$, $x_i \in Z$, $0 < x_i \leqslant p-1$, então $\Pi(\zeta_{p-1}) = x_1 \bmod p$. Provaremos em (1.32) que $x_1 \bmod p$ é gerador de $(Z/pZ)^*$; temos portanto um isomorfismo entre $<\zeta_{p-1}>$ e $(Z/pZ)^*$ pois $\Pi((\zeta_{p-1})^j) = (x_1 \bmod p)^j$. Definimos então $h : (Z/pZ)^* \longrightarrow Z_p^*$, $h((x_1 \bmod p)^j) = (\zeta_{p-1})^j$. Claramente h é um homomorfismo e $\Pi \circ h((x_1 \bmod p)^j) = \Pi((\zeta_{p-1})^j) = (x_1 \bmod p)^j$ qualquer $j \in Z$ e portanto $\Pi \circ h = id$.

Notamos assim que $1 \longrightarrow 1 + pZ_p \xrightarrow{i} Z_p^* \xrightarrow{\Pi} (Z/pZ)^*$ satisfaz a Proposição (1.30), logo $Z_p^* \simeq (1 + pZ_p) \times (Z/pZ)^*$ e con-

cluímos a prova de (1.26).

(1.32) Para provar que $x_1 \bmod p$ é gerador de $(Z/pZ)^*$, observemos que a ordem de $\Upsilon_{p-1} = (x_i \bmod p^i)_{i=1}^{\infty}$ em Z_p^* é igual a p-1; deste modo para todo i temos $(x_i \bmod p^i)^{p-1} = (x_i)^{p-1} \bmod p^i = 1$ em Z/p^iZ, ou equivalentemente, $(x_i)^{p-1} \equiv 1 \bmod p^i$. Suponhamos que $o(x_1 \bmod p) = k < p-1$, isto é, $(x_1)^k \equiv 1 \bmod p$; como $o(Z/pZ)^* = p-1$, temos $p-1 = k.t$ para algum $t \in Z_+$, $t \geqslant 2$. No Lema (1.2) provamos que $x_s \equiv x_r \bmod p^r$ para todo $s \geqslant r$, logo $(x_s)^k \equiv (x_r)^k \bmod p^r$; em particular, $(x_s)^k \equiv (x_1)^k \bmod p$, portanto $(x_s)^k \equiv 1 \bmod p$ e então $(x_s)^k = 1 + p.b$ para algum $b \in Z$. Por outro lado, $(x_s)^{p-1} \equiv 1 \bmod p^s$ e então $(x_s)^{p-1} = (x_s)^{k.t} = (1 + p.b)^t \equiv 1 \bmod p^s$; $(1 + p.b)^t =$

$$= \sum_{j=0}^{t} \binom{t}{j} . (p.b)^j = 1 + p.b. \sum_{j=1}^{t} \binom{t}{j} . (p.b)^{j-1} =$$

$$= 1 + p.b.(t + p.b. \sum_{j=2}^{t} \binom{t}{j} . (p.b)^{j-2}).$$

Como $2 \leqslant t < p-1 < p$, claramente $p \nmid u$, onde $u = t + p.b. \sum_{j=2}^{t} \binom{t}{j} . (p.b)^{j-2}$. Obtemos assim $(1 + p.b)^t = 1 + p.b.u \equiv 1 \bmod p^s$ e desde que $(u,p) = 1$, a congruência ocorre se e somente se $p^{s-1} \mid b$, ou seja, $b = p^{s-1}.w$ com $w \in Z$, e então $(x_s)^k = 1 + p.b = 1 + p^s.w$, consequentemente $(x_s)^k \equiv 1 \bmod p^s$, de modo que $o(x_s \bmod p^s) \leqslant k < p-1$ para todo $s \in Z_+$, portanto $o(\Upsilon_{p-1}) = k = o(x_1 \bmod p)$ e chegamos ao absurdo; assim $o(x_1 \bmod p) = p-1 = o(Z/pZ)^*$ e então $\langle x_1 \bmod p \rangle = (Z/pZ)^*$.

Para verificar (1.27), observemos que $Z_2^* = Z_2 - 2Z_2$; com isso chegamos a $Z_2^* = 1 + 2Z_2$, ou seja, $Z_2^* \simeq 1 + 2Z_2$.

Para provar que $1 + 2Z_2 \simeq \{\pm 1\} \times (1 + 4Z_2)$, seja

$1 \longrightarrow 1 + 4\mathbb{Z}_2 \xrightarrow{i} 1 + 2\mathbb{Z}_2 \xrightarrow{g} \{\pm 1\} \longrightarrow 1$ uma sequência com i = i-

dentidade; dado $x = (x_i \bmod 2^i)_{i=1}^{\infty} \in 1 + 2\mathbb{Z}_2$ definimos $g(x) = 1$ se

$x_2 \equiv 1 \bmod 4$ e $g(x) = -1$ se $x_2 \equiv -1 \bmod 4$ (isto é, $x_2 \equiv 3 \bmod 4$).

Claramente i e g são homomorfismos; além disso

$\operatorname{Im} i = 1 + 4\mathbb{Z}_2 = \ker g$ pois $x \in \ker g$ se e somente se $g(x) = 1$ e is-

so ocorre se e somente se $x \in 1 + 4\mathbb{Z}_2$; concluímos então que a sequên

cia é exata. Seja $h : \{\pm 1\} \longrightarrow 1 + 2\mathbb{Z}_2$ tal que $h(1) = (1 \bmod 2^i)_{i=1}^{\infty}$

e $h(-1) = (-1 \bmod 2^i)_{i=1}^{\infty}$. Claramente h é um homomorfismo e

$goh = id$ (pois $goh(1) = g((1 \bmod 2^i)_{i=1}^{\infty}) = 1$ e

$goh(-1) = g((-1 \bmod 2^i)_{i=1}^{\infty}$, portanto pela Proposição (1.30) temos

$1 + 2\mathbb{Z}_2 \cong \{\pm 1\} \times (1 + 4\mathbb{Z}_2)$.

§ 2 Construção do Critério

Esse parágrafo tem por objetivo demonstrar o Teorema (2.11) que na prática é o resultado mais importante desse trabalho, isso porque tal Teorema nos fornece um critério que decide se um número inteiro é primo ou não. Para sua aplicação são necessárias algumas condições que envolvem números inteiros p-ádicos e funções caracter, no entanto deixamos a análise da validade dessas condições para os parágrafos seguintes.

Explicitaremos agora resultados que serão utilizados no Teorema (2.11).

(2.1) Seja q um número primo e C o conjunto dos Números Complexos. Um caracter X módulo q é um homomorfismo de grupos de $(Z/qZ)^*$ em C^*. A imagem de X está contida em U_{q-1} que denotará o conjunto das raízes (q-1)-ésimas da unidade.

Uma função caracter pode ser vista como uma função de Z em C se definirmos $X(a) = X(a \bmod q)$ para todo $a \in Z$ e $X(0 \bmod q) = 0$.

Notando que q é um número primo, o anel Z/qZ é na verdade o corpo F_q e $(Z/qZ)^*$ é o grupo multiplicativo F_q^* que é cíclico de ordem q-1.

As proposições que vem a seguir nos fornecem alguns resultados sobre caracteres.

(2.2) PROPOSIÇÃO: O conjunto de todos os caracteres módulo q forma um grupo multiplicativo cíclico denotado por X_q e isomorfo a U_{q-1}.

PROVA: Seja $\chi: F_q^* \longrightarrow U_{q-1}$ com $\chi(g) = \zeta_{q-1}$ onde ζ_{q-1} é raiz q-1-ésima primitiva da unidade e g é gerador de F_q^*. χ é um caracter módulo q; mais ainda, χ é um isomorfismo entre F_q^* e U_{q-1}, visto que associa a cada $g^i \in F_q^*$ o elemento ζ_{q-1}^i de U_{q-1}. Claramente χ gera um grupo multiplicativo cíclico de ordem q-1 formado por χ^i, $0 \leqslant i \leqslant q-2$. χ^i também é caracter módulo q para todo $0 \leqslant i \leqslant q-2$, portanto $\{\chi^i: 0 \leqslant i \leqslant q-2\} \subset X_q$. Para concluirmos que $X_q = \{\chi^i: 0 \leqslant i \leqslant q-2\}$, seja $\varphi \in X_q$ tal que $\varphi(g) = \zeta_{q-1}^h$ para algum $h \in Z$; o Algorítmo de Euclides nos assegura que existe $i \in Z$, $0 \leqslant i \leqslant q-2$ tal que $h \equiv i \bmod (q-1)$ de modo que $\varphi = \chi^i$ e portanto $\varphi \in \{\chi^i: 0 \leqslant i \leqslant q-2\}$. Provamos assim que X_q é um grupo cíclico de ordem q-1. Por outro lado U_{q-1} também é um grupo cíclico de ordem q-1 e dois grupos cíclicos de mesma ordem são isomorfos. Nesse caso o isomorfismo pode ser obtido por

$\Psi: X_q \longrightarrow U_{q-1}$ com $\Psi(\chi^i) = \zeta_{q-1}^i$ para todo $i \in N$. ∎

(2.3) PROPOSIÇÃO: Sejam $x,y \in F_q^*$; se $\varphi(x) = \varphi(y)$ para todo $\varphi \in X_q$ então $x = y$.

PROVA: Se $\varphi(x) = \varphi(y)$ para todo $\varphi \in X_q$, em particular a igualdade vale para χ o gerador de X_q, ou seja $\chi(x) = \chi(y)$, observemos que $\varphi(x.y^{-1}) = 1$; no entanto χ é um isomorfismo de F_q^* em U_{q-1}, portanto $\chi(x.y^{-1}) = 1$ se e somente se $x = y$. ∎

Seja a decomposição de q-1 em fatores primos dada por:

(2.4) $q-1 = \prod_{p \text{ primo}} p^{k(p)}$ com $k(p) = v_p(q-1)$

Para cada primo p com $k(p) \geqslant 1$, seja $X_p k: F_q^* \longrightarrow U_p k$ tal que $X_p k(g) = \zeta_p k$, onde $0 \leqslant k \leqslant k(p)$, g é gerador de F_q^* e $\zeta_p k$ é raiz p^k-ésima primitiva da unidade. Para verificarmos que $X_p k$ é um caracter módulo q de ordem p^k, basta tomarmos $j = (q-1)/p^k$; assim $X_p k(g) = \zeta_p k = e^{2\pi i/p^k} = e^{(2\pi i/(q-1)).(q-1)/p^k} = e^{(2\pi i/(q-1))j}$ porém $(e^{2\pi i/(q-1)})^j = (\zeta_{q-1})^j = X^j(g)$, portanto $X_p k = X^j$ e X_q. A partir daqui $X_p k$ será denotado por $X_{p,q}$.

Apresentaremos agora um conjunto de geradores de X_q que será mais apropriado. Seja

(2.5) $\quad Y_q = \{X_{p,q} : p \text{ primo }, p/(q-1)\}$

(2.6) PROPOSIÇÃO: Y_q gera o grupo X_q.

PROVA: Já provamos que X_q é um grupo multiplicativo cíclico isomorfo a U_{q-1} e gerado por X, logo para todo $r \in \mathbb{Z}$, $(r,q-1) = 1$, X^r também é gerador de X_q. Desse modo, para provar que Y_q gera X_q basta construir algum X^r com $(r,q-1) = 1$ a partir de multiplicações de elementos de Y_q. Seja $\prod_{i=1}^{t} X_{p_i,q}$ o produto de todos os caracteres do conjunto Y_q e $r = \sum_{i=1}^{t} (q-1)/p_i^{k(p_i)}$ onde $k(p_i) = v_{p_i}(q-1)$. Para cada p primo com $p_i/(q-1)$ já verificamos anteriormente que $X_{p_i,q} = X^{(q-1)/p_i^{k(p_i)}}$; então $\prod_{i=1}^{t} X_{p_i,q} = \prod_{i=1}^{t} X^{(q-1)/p_i^{k(p_i)}} = X^r$. Por absurdo, seja $(r,q-1) = d$ com $d \neq 1$, de modo que existe algum $p_w/(q-1)$ tal que p_w/d e portanto p_w/r. Observemos que $r = \sum_{i=1}^{t} (q-1)/p_i^{k(p_i)} = \sum_{i=1}^{t} \prod_{\substack{j=1 \\ j\neq i}}^{t} p_j^{k(p_j)}$ pois $q-1 = \prod_{i=1}^{t} p_i^{k(p_i)}$, assim $r - \sum_{\substack{i=1 \\ i\neq w}}^{t} \prod_{\substack{j=1 \\ j\neq i}}^{t} p_j^{k(p_j)} = \prod_{\substack{j=1 \\ j\neq w}}^{t} p_j^{k(p_j)}$. Como p_w comparece em todos os produtos do primeiro membro da igualdade e p_w/r verificamos que

$p_w / (r - \sum_{\substack{i=1 \\ i \neq w}}^{t} \prod_{\substack{j=1 \\ j \neq i}}^{t} p_j^{k(p_j)})$, mas p_w não divide o segundo membro da igualdade e chegamos a um absurdo; logo $(r,q-1) = 1$ e X^r obtido a partir do produto de elementos de Y_q gera X_q. ∎

Dando prosseguimento provaremos a Proposição (2.8) que estabelece um critério para a validade da seguinte condição:

(2.7) $a^t \equiv 1 \bmod s$ para todo $a \in Z$, com $(a,s) = 1$

Para cada número inteiro positivo t, definiremos $e(t) = 2$ se t for ímpar e $e(t) = 2.\prod_{\substack{q \text{ primo} \\ (q-1)/t}} q^{v_q(t)+1}$ se t for par.

(2.8) PROPOSIÇÃO: Sejam s,t inteiros positivos com $s > 1$. A condição (2.7) é válida se e somente se $s/e(t)$.

PROVA: Faremos a prova primeiramente para t ímpar. Se a condição (2.7) vale, temos $a^t \equiv 1 \bmod s$ para todo $a \in Z$, $(a,s) = 1$; em particular para $a = -1$ temos $(-1)^t = -1 \equiv 1 \bmod s$, então $2 \equiv 0 \bmod s$; desde que, por hipótese $s \neq 1$, tal congruência ocorre se e somente se $s = 2$, portanto $s/e(t)$ visto que por definição $e(t) = 2$. Recíprocamente se $s/e(t)$ com $e(t) = 2$ temos $s = 2$ pois $s \neq 1$; então todo $a \in Z$ que satisfaz $(a,2) = 1$ é ímpar, de modo que a^t também é ímpar e consequentemente $a^t \equiv 1 \bmod s$.

Seja agora t um número par. Assumamos inicialmente que $s = q^m$ com q primo e $m \geq 1$. Se q for ímpar ou $m \leq 2$ então o grupo $(Z/q^mZ)^*$ é cíclico de ordem $(q-1).q^{m-1}$, assim se a condição (2.7) é satisfeita, em particular a congruência acontece para $g \in N$ onde g mod q^m é gerador de $(Z/q^mZ)^*$; obtemos então $g^t \equiv 1 \bmod q^m$, de modo que $(q-1).q^{m-1}/t$; consequentemente $(q-1)/t$ e $v_q(t) \geq m-1$. Note-

mos entretanto que $e(t) = 2.\prod_{\substack{(q-1)/t \\ q\ primo}} q^{v_q(t)+1}$ e que $v_q(t) + 1 \geqslant m$, assim $q^m/q^{v_q(t)+1}$ e como $s = q^m$, claramente $s/e(t)$. Recíprocamente se $q^m/e(t)$, da própria definição de $e(t)$ observamos que $(q-1)/t$ e q^{m-1}/t pois $v_q(t) + 1 \geqslant m$; como $(q,q-1) = 1$ temos $(q-1).q^{m-1}/t$ e concluímos que t é um múltiplo da ordem do grupo $(\mathbb{Z}/q^m\mathbb{Z})^*$, portanto $a^t \equiv 1 \bmod q^m$ para todo $a \in \mathbb{Z}$ com $(a,q) = 1$ e então a condição (2.7) é satisfeita para $s = q^m$.

Analisemos agora o caso $q = 2$ e $m \geqslant 3$. Se a condição (2.7) é satisfeita temos $a^t \equiv \bmod 2^m$ para todo $a \in \mathbb{Z}$, $(a,2) = 1$. Sabemos contudo que $(\mathbb{Z}/2^m\mathbb{Z})^* \simeq (\mathbb{Z}/2\mathbb{Z}) \otimes (\mathbb{Z}/2^{m-2}\mathbb{Z})$ onde $\mathbb{Z}/2^{m-2}\mathbb{Z}$ é cíclico; assim existe $c \bmod 2^{m-2} \in \mathbb{Z}/2^{m-2}\mathbb{Z}$ com ordem igual a 2^{m-2} e isso implica na existência de $b \bmod 2^m \in (\mathbb{Z}/2^m\mathbb{Z})^*$ também com ordem 2^{m-2}; logo, $b^t \equiv 1 \bmod 2^m$ de modo que $2^{m-2}/t$ e então $v_2(t) \geqslant m - 2$. Desde que $e(t) = 2.\prod_{\substack{(q-1)/t \\ q\ primo}} q^{v_q(t)+1}$, temos $2^{v_2(t)+2}/e(t)$, mas $v_2(t) + 2 \geqslant m$ o que implica em $2^m/e(t)$ portanto $s/e(t)$. Recíprocamente se $2^m/e(t)$ notamos que $2^m/2^{v_2(t)+2}$, logo $v_2(t) + 2 \geqslant m$ e então $2^{m-2}/t$. É fácil observar entretanto que qualquer elemento do grupo $(\mathbb{Z}/2^m\mathbb{Z})^*$ tem ordem divisível por 2^{m-2} de modo que $a^{2^{m-2}} \equiv 1 \bmod 2^m$ para todo $a \in \mathbb{Z}$, $(a,2) = 1$. Como t é múltiplo de 2^{m-2} claramente $a^t \equiv 1 \bmod 2^m$, isto é, $a^t \equiv 1 \bmod s$ para todo $a \in \mathbb{Z}$, $(a,s) = 1$.

Finalmente seja $s = \prod_{i=1}^{f} q_i^{m_i}$. Se a condição (2.7) é satisfeita temos $a^t \equiv 1 \bmod s$, logo $a^t \equiv 1 \bmod q_i^{m_i}$ para todo i, $1 \leqslant i \leqslant f$. Já verificamos no entanto que para $a^t \equiv 1 \bmod q_i^{m_i}$ temos $q_i^{m_i}/e(t)$, consequentemente $s/e(t)$. Recíprocamente se $s/e(t)$ provamos que $a^t \equiv 1 \bmod q_i^{m_i}$ para todo i, $1 \leqslant i \leqslant f$ e portanto

$a^t \equiv 1 \bmod \prod_{i=1}^{f} q_i^{m_i}$, ou seja, $a^t \equiv 1 \bmod s$. ■

A seguir, para efeito de completude do texto enunciaremos um teorema e um lema que serão utilizados na prova do Teorema (2.11).

(2.9) TEOREMA CHINÊS DE RESTOS: Dado o sistema de congruências

$x \equiv a_1 \bmod m_1$

.....

$x \equiv a_n \bmod m_n$ se $(m_i, m_j) = 1$ para $i \neq j$ então o sistema tem solução única.

PROVA: Oscar Zariski e Pierre Samuel - Commutative Algebra

Volume I - Capítulo V - Teorema 17

(2.10) LEMA: Seja q um número primo e $a \in \mathbb{Q}$ com $a \equiv 1 \bmod q$ e $a^{q-1} \equiv 1 \bmod q^m$; então $a \equiv 1 \bmod q^m$. (Dado $a \in \mathbb{Q}$, $a = m/n$ com $m,n \in \mathbb{Z}$, $(n,q) = 1$, definimos $a \bmod q = m \bmod q.(n \bmod q)^{-1}$).

PROVA: Seja $a = 1 + q.x/y$ com $x,y \in \mathbb{Z}$, $(y,q) = 1$; com isso $a^{q-1} = ((y + q.x)/y)^{q-1} = 1 + (1/y^{q-1}).\sum_{i=1}^{q-1}\binom{q-1}{i}.(q.x)^i.y^{q-1-i}$, logo $a^{q-1} - 1 = (q.x/y^{q-1}).((q - 1).y^{q-2} + x.q.\sum_{i=2}^{q-1}\binom{q-1}{i}.(q.x)^{i-2}.y^{q-1-i})$. Notemos que $q \nmid ((q - 1).y^{q-2} + x.q.\sum_{i=2}^{q-1}\binom{q-1}{i}.(q.x)^{i-2}.y^{q-1-i})$; assim $v_q(a^{q-1} - 1) = v_q(q.x/y^{q-1}) = 1 + v_q(x)$ pois $v_q(y) = 0$. Observemos no entanto que $a^{q-1} \equiv 1 \bmod q^m$ o que implica em $v_q(a^{q-1} - 1) \geqslant m$; assim $1 + v_q(x) \geqslant m$, portanto q^{m-1}/x, isto é, $x = q^{m-1}.s$ onde $s \in \mathbb{Z}$. Temos então $a = 1 + q.x/y = 1 + q^m.s/y$ com $(y,q) = 1$, consequentemente $a \equiv 1 \bmod q^m$. ■

Finalmente chegamos ao Teorema (2.11). As condições (2.12) e (2.13) que assumiremos nesse Teorema serão discutidas detalhadamente nos parágrafos seguintes.

(2.11) TEOREMA: Sejam t e s inteiros positivos satisfazendo $a^t \equiv 1 \bmod s$ para todo $a \in \mathbb{Z}$, $(a,s) = 1$ e seja n um inteiro satisfazendo $n > 1$, $s > \sqrt{n}$ e $(n, s.t) = 1$. Escrevemos $Y_s = \bigcup_{\substack{q/s \\ q \text{ primo}}} Y_q$ com $Y_q = \{X_{p,q} : p \text{ primo}, p/(q-1)\}$. Assumimos que qualquer primo p/t satisfaz a seguinte condição:

(2.12) { para qualquer r divisor primo de n existe $l_p(r) \in \mathbb{Z}_p$ tal que $r^{p-1} = (n^{p-1})^{l_p(r)}$ no grupo $1 + p\mathbb{Z}_p$.

Assumimos além disso que qualquer $X \in Y_s$ satisfaz a seguinte condição:

(2.13) { para qualquer r divisor primo de n nós temos $X(r) = X(n)^{l_p(r)}$ com $l_p(r)$ como em (2.12), onde p é tal que a ordem de X é potência de p.

Então para qualquer r divisor de n existe $i \in \{0,1,2,\ldots t-1\}$ tal que $r \equiv n^i \bmod s$.

Antes de procedermos a demonstração do teorema faremos algumas observações a respeito de seu significado. A partir de todas as condições satisfeitas o teorema nos assegura que para todo divisor r de n existe $i \in \{0,1,2\ldots t-1\}$ tal que $r \equiv n^i \bmod s$. Podemos então calcular $n^i \bmod s$ e em seguida verificar se r é divisor de n. Se os únicos divisores encontrados forem $r = 1$ e $r = n$ então n é primo; caso contrário n é composto.

Um aspecto que deve ser lembrado é o tempo que se leva para computar $n^i \bmod s$ com $i \in N$, $0 \leqslant i \leqslant t-1$, contudo essa computação pode ser feita rapidamente pois o t pode ser selecionado bastante pequeno em relação a n. Sua seleção pode ser feita através da Proposição (2.8); por exemplo, para testar n da ordem de 10^{18} é suficiente que t seja igual a 60 e para testar n da ordem de 10^{100} basta utilizar t = 5.054.

Outra observação que faremos aqui embora irrelevante para a demonstração do teorema nos parece interessante para a sua aplicação: esse teorema, que na verdade é um teste de primalidade, só é utilizado quando n é provavelmente primo, ou seja, antes de aplicá-lo n é submetido a testes de primalidade mais simples que revelam rapidamente, na maioria dos casos, se n é composto.

PROVA DO TEOREMA (2.11): Pelo fato da demonstração desse teorema ser extensa ela será dividida em algumas etapas. Observamos entretanto que durante toda a prova consideraremos apenas os divisores primos de n e somente no final verificaremos a validade dos resultados obtidos para os divisores genéricos de n.

A primeira etapa que vamos executar consiste em provar que para cada r divisor primo de n existe um número inteiro l(r) tal que $X_{p,q}(r) = X_{p,q}(n^{l(r)})$ qualquer que seja $X_{p,q} \in Y_s$.

Seja P o conjunto de todos os divisores primos de t. Para cada $p \in P$ existe um número inteiro h(p) suficientemente grande tal que

(2.14) $h(p) \geqslant \max\{\max\{v_p(q-1);\ q/s\};\ v_p(s)\}$

Seja $l'_p(r)$ um número inteiro tal que

(2.15) $l'_p(r) \equiv l_p(r) \bmod p^{h(p)}$ onde $l_p(r)$ é dado na condição (2.12).

Pelo Teorema Chinês de Restos: (2.9), existe $l(r) \in Z$ tal que $l(r) \equiv l'_p(r) \bmod p^{h(p)}$ para todo $p \in P$ e então por (2.15) obtemos

(2.16) $l(r) \equiv l_p(r) \bmod p^{h(p)}$ para todo $p \in P$.

Seja $U_p h(p)$ o grupo das raízes $p^{h(p)}$- ésimas da unidade; claramente $U_p h(p)$ é um grupo abeliano finito de ordem potência de p; dados $\zeta \in U_p h(p)$ e $a = (a_i \bmod p^i)_{i=1}^{\infty} \in Z_p$ definimos no §1 (conferir (1.4)) o elemento ζ^a como $\zeta^a{}_m$ para m suficientemente grande; concluímos então que $\zeta_{p^{h(p)}}^{l_p(r)} = \zeta_{p^{h(p)}}^{l(r)}$ pois $l(r) \equiv l_p(r) \bmod p^{h(p)}$. Utilizando agora a condição (2.13) temos $X(r) = X(n)^{l_p(r)}$ para todo $X \in Y_s$, assim $X_{p,q}(r) = X_{p,q}(n)^{l_p(r)}$. No entanto $X_{p,q} : F_q^* \longrightarrow U_p k(p)$ e $U_p k(p) \subset U_p h(p)$ visto que $v_p(q-1) = k(p) \leqslant h(p)$ de modo que $X_{p,q}(n) \in U_p h(p)$ e então $X_{p,q}(n)^{l_p(r)} = X_{p,q}(n)^{l(r)}$; observemos entretanto que $l(r) \in Z$ e que $X_{p,q}$ é homomorfismo, consequentemente $X_{p,q}(n)^{l(r)} = X_{p,q}(n^{l(r)})$, ou seja, $X_{p,q}(r) = X_{p,q}(n)^{l_p(r)} = X_{p,q}(n)^{l(r)} = X_{p,q}(n^{l(r)})$ para todo $X_{p,q} \in Y_s$, portanto $X(r) = X(n^{l(r)})$ para todo $X \in Y_s$.

Dando prosseguimento, o próximo passo será provar que para cada primo q fixado, se q/s temos

(2.17) $r \equiv n^{l(r)} \bmod q^{m(q)}$ onde $m(q) = v_q(s)$

Se $m(q) = 1$ a congruência anterior será facilmente verificada pois $X(r) = X(n^{l(r)})$ para todo $X \in Y_s$ e Y_s gera X_q de modo que $\varphi(r) = \varphi(n^{l(r)})$ para todo $\varphi \in X_q$; no entanto provamos na Proposição (2.3) que dados $x,y \in F_q^*$ se $\varphi(x) = \varphi(y)$ para todo $\varphi \in X_q$ então $x = y$, portanto

(2.18) $r \equiv n^{l(r)} \bmod q$

e a congruência (2.17) é satisfeita.

Se $m(q) \geqslant 2$ provaremos que $r^{q-1} \equiv (n^{q-1})^{l(r)} \bmod q^{m(q)}$ e em seguida construiremos $a = r.n^{-l(r)}$ que vai satisfazer a congruência $a \equiv 1 \bmod q$. A partir das duas congruências obteremos (2.17).

Utilizando (2.14) temos $h(q) \geqslant v_q(s)$; então $v_q(s) = m(q) > m(q) - 1$ de modo que $h(q) = m(q) - 1 + x$ com $x \in N$; assim $(n^{q-1})^{q^{h(q)}} = ((n^{q-1})^{q^{m(q)-1}})^{q^x}$. Notemos no entanto que a ordem do grupo $(Z/q^{m(q)}Z)^*$ é $(q-1).q^{m(q)-1}$ portanto $n^{(q-1).q^{m(q)-1}} \equiv 1 \bmod q^{m(q)}$ e então

(2.19) $(n^{q-1})^{q^{h(q)}} \equiv 1 \bmod q^{m(q)}$

Por (2.16) temos $l(r) \equiv l_q(r) \bmod q^{h(q)}$, isto é, $l_q(r) = l(r) + q^{h(q)}.y$ com $y \in Z_q$; daí

(2.20) $(n^{q-1})^{l_q(r)} = (n^{q-1})^{l(r)}.((n^{q-1})^{q^{h(q)}})^y$

Por (2.19): $(n^{q-1})^{q^{h(q)}} \equiv 1 \bmod q^{m(q)}$ e então $(n^{q-1})^{q^{h(q)}}$ pode ser visto como um elemento de $1 + qZ_q$ que é um Z_q-módulo (conferir (1.16)) de modo que $((n^{q-1})^{q^{h(q)}})^y$ também é um elemento de $1 + qZ_q$ para todo $y \in Z_q$.

De (2.19): $(n^{q-1})^{q^{h(q)}} \equiv 1 \bmod q^{m(q)}$ obtemos $((n^{q-1})^{q^{h(q)}})^y \equiv 1 \bmod q^{m(q)}$ e a partir de (2.20) encontramos

(2.21) $(n^{q-1})^{l_q(r)} \equiv (n^{q-1})^{l(r)} \mod q^{m(q)}$

Observemos agora t e s. Por construção t é par; recorrendo a Proposição (2.8): s/e(t); lembrando que $v_q(s) = m(q)$ e $e(t) = 2.\prod_{\substack{(q-1)/t \\ q \text{ primo}}} q^{v_q(t)+1}$ verificamos que $q^{m(q)}/e(t)$, assim, se $q = 2$ claramente q/t e se $q \neq 2$, $q^{m(q)}/q^{v_q(t)+1}$ e então $2 \leqslant m(q) \leqslant v_q(t) + 1$, portanto $v_q(t) \geqslant 1$. Concluímos daí que se $m(q) \geqslant 2$ então q/t e por hipótese q está nas condições de um número primo que satisfaz (2.12), logo para o $l_q(r)$ usado na condição (2.12) temos $r^{q-1} = (n^{q-1})^{l_q(r)}$ em $1 + qZ_q$. Substituindo esse valor em (2.21) obtemos

(2.22) $r^{q-1} \equiv (n^{q-1})^{l(r)} \mod q^{m(q)}$

Seja agora $a = r.n^{-l(r)}$ e Z_q.

Em (2.18) obtivemos $r \equiv n^{l(r)} \mod q$, mas $l(r) \in Z$ e $(n,q) = 1$, assim $n^{l(r)} \in Q$ e $n^{l(r)} \mod q \in Z/qZ$; observemos no entanto que $(r,q) = 1$ de modo que $r \not\equiv 0 \mod q$ e então $n^{l(r)} \not\equiv 0 \mod q$ o que implica em $n^{l(r)} \mod q \in (Z/qZ)^*$, logo $n^{l(r)} \mod q$ possui inverso em Z/qZ, então $r.n^{-l(r)} \equiv 1 \mod q$ ou equivalentemente

(2.23) $a \equiv 1 \mod q$

Por outro lado, desde que $(q,n) = 1$ e $l(r), q - 1 \in Z$, $(n^{q-1})^{-l(r)} \mod q^{m(q)} \in (Z/q^{m(q)}Z)^*$ e a partir de (2.22) obtemos $r^{q-1}.(n^{q-1})^{-l(r)} \equiv 1 \mod q^{m(q)}$, assim $(r.n^{-l(r)})^{q-1} \equiv 1 \mod q^{m(q)}$, ou equivalentemente

(2.24) $a^{q-1} \equiv 1 \mod q^{m(q)}$

Combinando (2.23) com (2.24) obtemos do Lema (2.10) a congruência $a \equiv 1 \mod q^{m(q)}$, portanto $r \equiv n^{l(r)} \mod q^{m(q)}$ e (2.17)

está provado para todo q divisor de s.

Como $m(q) = v_q(s)$, $s = \prod_{q|s} q^{m(q)}$ temos $r \equiv n^{l(r)} \bmod s$.

Por hipótese $n^t \equiv 1 \bmod s$, e fazendo $l(r) = t.x + i$ com $x, i \in \mathbb{Z}$, $0 \leqslant i < t$ obtemos $n^{l(r)} = (n^t)^x . n^i \equiv n^i \bmod s$ e portanto $r \equiv n^i \bmod s$ com $0 \leqslant i < t$. ∎

§ 3 Viabilidade do Critério

Como vimos no parágrafo anterior a aplicação de Teorema (2.11) depende da validade das hipóteses (2.12) e (2.13). Nesse parágrafo além de analisarmos algumas condições para que (2.12) ocorra provaremos também o Teorema (3.21) que nos dá condições para a validade de (2.13) de modo a podermos utilizar o Teorema (2.11) e decidir se n é primo ou não.

Faremos agora algumas afirmações necessárias para o desenvolvimento deste parágrafo, porém algumas provas serão omitidas por tratarem de relações elementares de teoria de grupos, anéis e corpos.

Seja ζ_m uma raiz m-ésima primitiva da unidade. As raízes m-ésimas da unidade formam um grupo multiplicativo cíclico denotado por U_m, gerado por ζ_m (conferir (2.2)).

Fixemos agora os primos q,p e também seja fixado $k \in N^*$ tal que $p^k/(q-1)$.

(3.1) Seja $A = \mathbb{Z}[\zeta_p{}^k, \zeta_q]$ o anel gerado por $\zeta_p{}^k$ e ζ_q e seja $K = Q(\zeta_p{}^k, \zeta_q)$ seu corpo de frações. Afirmamos que todo elemento de K tem representação única como $\sum_{\substack{0 \le i \le p^k-1 \\ 0 \le j \le q-1}} a_{ij} \cdot (\zeta_p{}^k)^i \cdot (\zeta_q)^j$ com $a_{ij} \in Q$.

(3.2) Denotemos por B o subanel de K tal que $B = A\left[\frac{1}{q}\right]$.

É fácil observar que um elemento de K pertence a B se e somente se os denominadores de todos os coeficientes a_{ij} são potências de q.

Dado $x \in \mathbb{Z}$, $x \not\equiv 0 \bmod p$, seja $\sigma_x : K \longrightarrow K$ o automorfismo tal que $\sigma_x(\zeta_p k) = (\zeta_p k)^x$ e $\sigma_x(\zeta_q) = \zeta_q$.

$G = \{\sigma_x : 1 \leqslant x \leqslant p^k,\ x \not\equiv 0 \bmod p\}$ é o grupo de Galois de K sobre $\mathbb{Q}(\zeta_q)$ e G é isomorfo a $(\mathbb{Z}/p^k\mathbb{Z})^*$.

Seja $\mathbb{Z}[G]$ o anel de grupo.

(3.3) Para $u \in B^*$ e $\alpha = \sum_{\sigma \in G} n_\sigma \sigma \in \mathbb{Z}[G]$, definimos $u^\alpha \in B^*$ como $u^\alpha = \prod_{\sigma \in G} \sigma(u)^{n_\sigma}$

Essas operações de $\mathbb{Z}[G]$ sobre B^* satisfazem:

(3.4) $(u.v)^\alpha = u^\alpha . v^\alpha$

(3.5) $u^{\alpha.\beta} = (u^\alpha)^\beta$

(3.6) $u^{\alpha+\beta} = u^\alpha . v^\beta$

(3.7) $u^1 = u$

e fazem de B^* um $\mathbb{Z}[G]$-módulo.

Seja $X : (\mathbb{Z}/q\mathbb{Z})^* \longrightarrow \langle \zeta_p k \rangle$ função caracter de ordem p^k, isto é, $X(g) = \zeta_p k$ para g gerador de $(\mathbb{Z}/q\mathbb{Z})^*$. Como já vimos no §2 a função caracter pode ser vista como uma função de $\mathbb{Z}$ em C se definirmos $X(a) = X(a \bmod q)$ para todo $a \in \mathbb{Z}$ e $X(0 \bmod q) = 0$; no entanto se identificarmos $X(a^{-1})$ com $X((a \bmod q)^{-1})$ para $a \not\equiv 0 \bmod q$, podemos ir mais além e definir $X(a^{-1}) = X(a)^{-1}$ para todo $a \in \mathbb{Z}$ e $(a,q) = 1$ pois todo elemento $X(a) \in \langle \zeta_p k \rangle$ possui inverso .

(3.8) Definimos a Soma de Gauss $T(X)$ associada a X como $T(X) = \sum_{x=1}^{q-1} X(x).(\zeta_q)^x$.

Claramente $T(X) \in \Lambda = \mathbb{Z}[\zeta_p k, \zeta_q]$.

Provaremos a seguir que

(3.9) $T(X).T(X^{-1}) = X(-1).q$

utilizando o seguinte lema:

(3.10) LEMA: a) $T(\overline{X}) = X(-1).\overline{T(X)}$

b) $T(X).\overline{T(X)} = q$

c) $T(X).T(\overline{X}) = X(-1).q$

PROVA: Para demonstrar a primeira parte do Lema denotemos por ζ_r uma raiz r-ésima da unidade; $\zeta_r = \cos 2.\pi/r + i.\text{sen } 2.\pi/r$, de modo que o seu conjugado $\overline{\zeta}_r$ é igual a $\cos 2.\pi/r - i.\text{sen } 2.\pi/r$; obtemos então $\zeta_r.\overline{\zeta}_r = 1$, logo

(3.11) $\overline{\zeta_r} = (\zeta_r)^{-1}$

Do resultado acima concluímos que $\overline{X(x)} = X(x)^{-1}$ para todo x mod q $\in (Z/qZ)^*$ pois $X(x) \in \langle \zeta_p k \rangle$; no entanto $-x = (q - x) - q$ de modo que $-x \equiv (q - x) \bmod q$ e daí obtemos $(\zeta_q)^{-x} = (\zeta_q)^{q-x}$ e $X(-x) = X(q-x)$, logo $X(x)' = X(-1).X(q-x)$ e então $\overline{T(X)} = \sum_{x=1}^{q-1} X(x)^{-1}.(\zeta_q)^{-x} = X(-1)^{-1}.\sum_{x=1}^{q-1} X(q-x)^{-1}.(\zeta_q)^{q-x}$; assim, fazendo troca de variáveis e reordenando a somatória obtemos $\overline{T(X)} = X(-1)^{-1}.\sum_{x=1}^{q-1} X(x)^{-1}.(\zeta_q)^{x} = X(-1)^{-1}.\sum_{x=1}^{q-1} \overline{X(x)}.(\zeta_q)^{x}$ e então obtemos $\overline{T(X)} = X(-1)^{-1}.T(\overline{X})$, ou equivalentemente, $T(\overline{X}) = X(-1).\overline{T(X)}$.

Para provar o ítem b) do Lema, sejam $T(X) = \sum_{a=1}^{q-1} X(a).(\zeta_q)^{a}$ e $\overline{T(X)} = \sum_{b=1}^{q-1} X(b)^{-1}.(\zeta_q)^{-b} = \sum_{b=1}^{q-1} X(b^{-1}).(\zeta_q)^{-b}$ logo $T(X).\overline{T(X)} = \sum_{a=1}^{q-1}\sum_{b=1}^{q-1} X(a.b^{-1}).(\zeta_q)^{a-b}$. Para cada b fixado seja $c \equiv a.b^{-1} \bmod q$, assim $X(c) = X(a.b^{-1})$ e $a \equiv b.c \bmod q$, logo $(\zeta_q)^{a} = (\zeta_q)^{b.c}$ e então $(\zeta_q)^{a-b} = (\zeta_q)^{a}.(\zeta_q)^{-b} = (\zeta_q)^{b.c}.(\zeta_q)^{-b} =$

$= (\zeta_q)^{b.(c-1)}$, portanto $T(X).\overline{T(X)} = \sum_{c=1}^{q-1} X(c).\sum_{b=1}^{q-1}(\zeta_q)^{b.(c-1)}$.

Analisando c = 1 encontraremos $X(1).\sum_{b=1}^{q-1}(\zeta_q)^{b.(1-1)} = X(1).\sum_{b=1}^{q-1} 1 = q - 1$. Sabemos no entanto que $\sum_{x=0}^{q-1}(\zeta_q)^x = 0$ visto que essa igualdade corresponde a soma das raízes do polinômio $P(Y) = Y^q - 1$, então $\sum_{x=1}^{q-1}(\zeta_q)^x = -1$ e consequentemente $\sum_{b=1}^{q-1}(\zeta_q)^{b.(c-1)} = -1$ pois quando b percorre $W = \{w \in Z : 1 \leqslant w \leqslant q-1\}$ $b.(c-1) \bmod q$ percorre $(Z/qZ)^*$ para cada $c \neq 1$.

Das relações acima obtemos

(3.12) $T(X).\overline{T(X)} = q - 1 - \sum_{c=2}^{q-1} X(c)$

Seja agora $\bar{g}$ gerador de $(Z/qZ)^*$, onde $\bar{g} \equiv g \bmod q$ para $g \in Z$, logo para todo $c_1 \bmod q \neq c_2 \bmod q$ em $(Z/qZ)^*$ existe $i_1 \neq i_2$, $0 \leqslant i_1 \leqslant q - 2$, $0 \leqslant i_2 \leqslant q - 2$ tal que $c_1 \bmod q = (\bar{g})^{i_1}$, $c_2 \bmod q = (\bar{g})^{i_2}$ de modo que $\sum_{c=1}^{q-1} X(c) = \sum_{i=0}^{q-2} X(g^i) = \sum_{i=0}^{q-2} X(g)^i$. Claramente $\sum_{i=0}^{p^k-1} X(g)^i = 0$ pois $X(g) = \zeta_p k$. Como $p^k/(q-1)$ temos $q - 1 = w.p^k$, logo $\sum_{i=0}^{q-2} X(g)^i = \sum_{i=0}^{p^k-1} X(g)^i + \sum_{i=p^k}^{2.p^k-1} X(g)^i + \ldots\ldots + \sum_{i=(w-1).p^k}^{w.p^k-1} X(g)^i$ e portanto $\sum_{i=0}^{q-2} X(g)^i = 0$ o que se deve ao fato de todas as somatórias serem iguais a 0. Notamos assim que $\sum_{c=1}^{q-1} X(c) = \sum_{i=0}^{q-2} X(g)^i = 0$; mas $1 = X(1) = X(g)^0$ logo $\sum_{c=2}^{q-1} X(c) = -1$. Substituindo o valor acima em (3.12) encontramos $T(X).\overline{T(X)} = q - 1 - (-1) = q$ e assim provamos o ítem b).

A partir de a) e b) obtemos c) facilmente: por a) temos $\overline{T(X)} = X(-1)^{-1}.T(\bar{X})$; substituindo $\overline{T(X)}$ em b) encontramos $T(X).\overline{T(X)} = T(X).X(-1)^{-1}.T(\bar{X}) = q$ e então $T(X).T(\bar{X}) = X(-1).q$ o que prova o Lema. ∎

Para verificarmos que (3.9) é equivalente ao ítem c) do

Lema (3.10), notemos que $\overline{X} = X^{-1}$ e então $T(X).T(\overline{X}) = X(-1).q$ equivale a $T(X).T(X^{-1}) = X(-1).q$ e a igualdade (3.9) está demonstrada.

Nosso próximo passo será provar o Lema (3.13) cujo corolário será utilizado na demonstração do Teorema (3.21).

(3.13) LEMA: Se n é um número primo então $T(X)^{n-\sigma_n} \equiv X(n)^{-n} \mod nB$.

PROVA: Para checar que $T(X)^{n-\sigma_n}$ faz sentido observemos que por (3.9) $T(X)^{-1} = (X(-1).T(X^{-1}))/q$ e então $T(X)^{-1} \in B^*$ onde $B = Z[\zeta_p k, \zeta_q][1/q]$, mas $T(X) \in B$, o que implica em $T(X)$ pertencer a B^* e de acordo com a definição (3.3) podemos calcular $T(X)^{n-\sigma_n}$.

Para demonstrar o Lema utilizaremos o seguinte resultado:

Para n primo, então para todo anel comutativo R nós temos $(a + b)^n \equiv (a^n + b^n) \mod nR$ para todo $a,b \in R$; a congruência ocorre porque os coeficientes binomiais $\binom{n}{i}$ para $1 \leq i \leq n-1$ são divisíveis por n.

Observamos então que $T(X)^n \equiv \sum_{x=1}^{q-1} X(x)^n.(\zeta_q)^{n.x} \mod nB$ e como $q \nmid n$, $X(n) \neq 0$ de modo que podemos multiplicar e dividir o segundo lado da congruência por $X(n)^n$ encontrando $T(X)^n \equiv (1/X(n)^n).\sum_{x=1}^{q-1} X(n.x)^n.(\zeta_q)^{n.x} \mod nB$. Se fizermos $y \equiv n.x \mod q$ notaremos que quando x percorre o conjunto $W = \{w \in Z : 1 \leq w \leq q-1\}$, y também percorre W, portanto, $T(X)^n \equiv X(n)^{-n}.\sum_{y=1}^{q-1} X(y)^n.(\zeta_q)^y \mod nB$. Vejamos ainda que $X(y)^n = \sigma_n(X(y))$ e $(\zeta_q)^y = \sigma_n((\zeta_q)^y)$, então $\sum_{y=1}^{q-1} X(y)^n.(\zeta_q)^y = \sigma_n(\sum_{y=1}^{q-1} X(y).(\zeta_q)^y) = \sigma_n(T(X))$. Consequentemente

$T(X)^n \equiv X(n)^{-n}.T(X)^{\sigma_n} \bmod nB$. Já verificamos no entanto que $T(X)$ possui inverso em B, logo $T(X)^{n-\sigma_n} \equiv X(n)^{-n} \bmod nB$ e o Lema está provado. ∎

(3.14) COROLÁRIO: Se n é primo, então $T(X)^{(n-\sigma_n).\beta} \equiv X(n)^{-n.\beta} \bmod N$ para todo $\beta \in Z[G]$ e todo ideal N de B com $n \in N$.

PROVA: Do lema anterior $X(n)^n.T(X)^{n-\sigma_n} \equiv 1 \bmod nB$ com $T(X)^{n-\sigma_n} \in B^*$ e $X(n)^n \in B^*$, assim podemos calcular $(X(n)^n.T(X)^{n-\sigma_n})^\beta \equiv 1^\beta \bmod nB$ e utilizando (3.4) e (3.5) obtemos $X(n)^{n.\beta}.T(X)^{(n-\sigma_n).\beta} \equiv 1 \bmod nB$. Por outro lado N é ideal de B e $n \in N$ logo $nB \subset N$ e assim temos $X(n)^{n.\beta}.T(X)^{(n-\sigma_n).\beta} \equiv 1 \bmod N$, ou equivalentemente, $T(X)^{(n-\sigma_n).\beta} \equiv X(n)^{-n.\beta} \bmod N$. ∎

Dando prosseguimento, enunciaremos agora mais alguns resultados preparatórios para o Teorema (3.21), entre eles duas condições necessárias para a sua aplicação.

Sejam $\beta \in Z[G]$ e N ideal de B tal que:

(3.15) $(\zeta_p)^\beta \neq 1$

(3.16) $N \cap Z = nZ$ e $\sigma_n[N] = N$

Notemos que $\beta = 1$ satisfaz (3.15) e $N = nB$ satisfaz (3.16). Observemos também que:

(3.17) PROPOSIÇÃO: Seja $I = \{x \in Z : 1 \leqslant x \leqslant p^k;\ x \not\equiv 0 \bmod p\}$. Se $\beta = \sum_{x \in I} n_x.\sigma_x \in Z[G]$ então $(\zeta_p)^\beta \neq 1$ é equivalente a

$\sum_{x\in I} n_x.x \not\equiv 0 \bmod p$.

PROVA: Sabemos que $(\zeta_p k)^{p^{k-1}} = \zeta_p$ de modo que $\zeta_p \in \langle \zeta_p k\rangle$ e então $\sigma_x(\zeta_p) = (\zeta_p)^x$ para todo $x \in I$, logo $(\zeta_p)^\beta = \prod_{x\in I}\sigma_x(\zeta_p)^{n_x} = \prod_{x\in I}(\zeta_p)^{x.n_x}$, assim $(\zeta_p)^\beta = (\zeta_p)^{\sum_{x\in I} x.n_x}$ onde $\sum_{x\in I} x.n_x \in \mathbb{Z}$, portanto $(\zeta_p)^{\sum_{x\in I} x.n_x} \neq 1$ se e somente se p não divide $\sum_{x\in I} x.n_x$ o que implica em $(\zeta_p)^\beta \neq 1$ se e somente se $\sum_{x\in I} x.n_x \not\equiv 0 \bmod p$. ∎

Outro resultado que nos interessa é o seguinte:

(3.18) PROPOSIÇÃO: Se $(\zeta_p)^\beta \neq 1$ então $\varphi : U_p k \longrightarrow U_p k$ com $\varphi(\zeta) = \zeta^\beta$ qualquer $\zeta \in U_p k$ é um automorfismo.

PROVA: Claramente φ é uma função. Para constatar o homomorfismo sejam ζ_1, $\zeta_2 \in U_p k$ e I, como na proposição anterior. De acordo com (3.4): $(u.v)^\alpha = u^\alpha.v^\alpha$ para $u,v \in B^*$, $\alpha \in \mathbb{Z}[G]$, portanto $\varphi(\zeta_1.\zeta_2) = \varphi(\zeta_1).\varphi(\zeta_2)$. Para verificar que φ é injetiva suponhamos que $\zeta \in \operatorname{Ker}\varphi$ e a ordem de ζ seja igual a p^r com $r \neq 0$, então $(\zeta^{p^{r-1}})^p = 1$, portanto $\zeta^{p^{r-1}}$ é uma raíz p-ésima primitiva da unidade. Como $\zeta \in \operatorname{Ker}\varphi$ temos $\varphi(\zeta) = \zeta^\beta = 1$, logo $(\zeta^\beta)^{p^{r-1}} = 1$ e obtemos $(\zeta^{p^{r-1}})^\beta = (\zeta_p)^\beta = 1$ o que é absurdo pois por hipótese $(\zeta_p)^\beta \neq 1$. Assim $\zeta \in \operatorname{Ker}\varphi$ se e somente se $\zeta = 1$ e então φ é injetiva. Como $U_p k$ é finito e φ é injetiva então φ é sobrejetiva e isso conclui a prova. ∎

Demonstraremos agora uma proposição bastante simples cujo resultado será utilizado na prova do Teorema (3.21).

(3.19) PROPOSIÇÃO: Seja A um anel, I um ideal e $\sigma : A \longrightarrow A$ automorfismo de A tal que $\sigma[I] = I$. Dados $a,b \in A$, se $a \equiv b \bmod I$ então $\sigma(a) \equiv \sigma(b) \bmod I$.

PROVA: Se $a \equiv b \bmod I$ então $a = b + i$ com $i \in I$ logo $\sigma(a) = \sigma(b + i) = \sigma(b) + \sigma(i)$, mas por hipótese $\sigma(i) \in I$ portanto $\sigma(a) \equiv \sigma(b) \bmod I$. ∎

O último resultado preliminar necessário para a demonstração do Teorema (3.21) é o seguinte:

(3.20) LEMA: Seja r um divisor primo de n, $r \neq 1$ e seja o ideal $R = r B + N$ com N satisfazendo a condição (3.16). Se $\zeta \in U_{p^k}$ satisfaz $\zeta \equiv 1 \bmod R$ então $\zeta = 1$.

PROVA: Seja $P(Y) = Y^{p^k} - 1 = \prod_{\zeta \in U_{p^k}} (Y - \zeta)$. Sabemos que $(Y^{p^k} - 1)/(Y - 1) = \sum_{i=0}^{p^k-1} Y^i$ portanto $\prod_{\substack{\zeta \in U_{p^k} \\ \zeta \neq 1}} (Y - \zeta) = \sum_{i=0}^{p^k-1} Y^i$. Substituindo na última expressão x por 1 encontraremos $\prod_{\substack{\zeta \in U_{p^k} \\ \zeta \neq 1}} (1 - \zeta) = \sum_{i=0}^{p^k-1} 1 = p^k$. Se supusermos que esse Lema não é verdadeiro, existe $\zeta \in U_{p^k}$, $\zeta \neq 1$ tal que $\zeta \equiv 1 \bmod R$, ou seja, $(1 - \zeta) \in R$ o que implica em $\prod_{\zeta \neq 1} (1 - \zeta) \in R$ pois R é ideal de B. Concluímos então que $p^k \in R$ com $R = r B + N$ e assim $p^k = r.x + y$ com $x \in B$ e $y \in N$. Como r é divisor de n temos $n/r \in Z \subset B$, logo $(n/r).p^k \in R$, isto é, $n.x + (n/r).y \in R$. Notemos agora que N é um ideal de B com $n \in N$ e $y \in N$, então $n.x + (n/r).y \in N$, ou seja, $(n/r).p^k \in N$ e por (3.16): $N \cap Z = nZ$ de modo que $(n/r).p^k \in nZ$ o que é possível se e somente se $p^k/r \in Z$, ou equivalentemente, r divide p^k; no entanto r não divide p^k pois r é divisor de n e $(n,p) = 1$. Chegamos

assim a uma contradição, portanto o Lema é verdadeiro. ∎

(3.21) TEOREMA: Seja $X : F_q^* \longrightarrow U_p k$ tal que $X(g) = \zeta_p k$, onde g é gerador de F_q^*. Assumamos que:

(3.22) $\begin{cases} T(X)^{(n-\sigma_n)\cdot\beta} \equiv \zeta \bmod N \text{ para algum } \zeta \in U_p k, \text{ algum } \beta \text{ satisfazendo (3.15) e algum ideal } N \text{ de } B \text{ satisfazendo (3.16).} \end{cases}$

Assumamos adicionalmente que (2.12) é satisfeita. Então X satisfaz (2.13), isto é, $X(r) = X(n)^{l_p(r)}$ para todo divisor r de n, com $l_p(r)$ como em (2.12).

PROVA: Faremos a demonstração desse Teorema em várias etapas por ela ser longa e o desenvolvimento dos diversos passos sem uma explicitação mais clara pode tornar a prova um pouco confusa. Aproveitamos salientar aqui que todas as hipóteses desse Teorema são impressindíveis para sua validade.

Usaremos a notação $T(X)^{\beta} = u$ para evitar sobrecarga de símbolos.

A primeira etapa da prova consiste em fazer uma série de modificações em (3.22) a fim de encontrarmos uma nova congruência módulo N válida para todo $i \in \mathbb{Z}_+$. Em seguida veremos que dado um número primo r, a congruência (3.22) é válida se substituirmos n por r, ζ por $X(r)^{-r\cdot\beta}$ e N por rB de modo que todas as modificações feitas em (3.22) podem ser realizadas com esses novos valores.

Seja $I = \{x \in \mathbb{Z} : 1 \leqslant x \leqslant p^k;\ x \not\equiv 0 \bmod p\}$ e $\beta = \sum_{x\in I} n_x \cdot \sigma_x$ com $n_x \in \mathbb{Z}$. Por hipótese β satisfaz (3.15), ou seja, $\zeta_p^{\beta} \neq 1$. De acordo com (3.17), $\zeta_p^{\beta} \neq 1$ é equivalente a $\sum_{x\in I} x.n_x \not\equiv 0 \bmod p$; como

$(n,p) = 1$, claramente $-n.\sum_{x\in I} x.n_x \not\equiv 0 \bmod p$, logo $(\zeta_p)^{-n.\beta} \neq 1$. Assim, pela Proposição (3.18) $\Psi : \eta \longrightarrow \eta^{-n.\beta}$ é um automorfismo de grupo de $U_p k$, portanto $\zeta = \eta^{-n.\beta}$ para algum $\eta \in U_p k$. Podemos então substituir ζ por $\eta^{-n.\beta}$ em (3.22) obtendo

(3.23) $u^{n-\sigma_n} = \eta^{-n.\beta} \bmod N$

Sabemos no entanto que $z^k - y^k = (z - y).\sum_{j=0}^{k-1} z^{k-1-j}.y^j$; de modo que

(3.24) $(n - \sigma_n).\sum_{j=0}^{i-1} n^{i-1-j}.(\sigma_n)^j = n^i - (\sigma_n)^i$

Notemos agora que $\eta^{\sigma_n} = \eta^n$, logo

(3.25) $\eta^{-n.\beta.\sum_{j=0}^{i-1} n^{i-1-j}.(\sigma_n)^j} = \eta^{-n.\beta.\sum_{j=0}^{i-1} n^{i-1}} = \eta^{-i.n^i.\beta}$

Do fato de $\sigma_n[N] = N$ e pela Proposição (3.19) nos é permitido elevar os dois lados da congruência (3.23) a $\sum_{j=0}^{i-1} n^{i-1-j}.(\sigma_n)^j$, obtendo $(u^{n-\sigma_n})^{\sum_{j=0}^{i-1} n^{i-1-j}.(\sigma_n)^j} \equiv \eta^{-n.\beta.\sum_{j=0}^{i-1} n^{i-1-j}.(\sigma_n)^j} \bmod N$. Recorrendo a (3.24) e (3.25) encontramos

(3.26) $u^{n^i-(\sigma_n)^i} \equiv \eta^{-i.n^i.\beta} \bmod N$ para todo $i \in \mathbb{Z}_+$

Em particular, se tomarmos $i = (p - 1).p^k$ a congruência acima se transforma em $u^{n^{(p-1).p^k}-(\sigma_n)^{(p-1).p^k}} \equiv \eta^{-(p-1).p^k.n^{(p-1).p^k}.\beta} \bmod N$. Notamos contudo que $\eta \in U_p k$ e a ordem de $U_p k$ é p^k, dessa forma $-(p - 1).p^k.n^{(p-1).p^k}$ é múltiplo da ordem do grupo de modo que $(\eta^{-(p-1).p^k.n^{(p-1).p^k}})^\beta = 1^\beta = 1$; então a congruência acima se torna $u^{n^{(p-1).p^k} - (\sigma_n)^{(p-1).p^k}} \equiv 1 \bmod N$. Por outro lado $\sigma_n \in G$ com $G \simeq (\mathbb{Z}/p^k\mathbb{Z})^*$ cuja ordem é $(p - 1).p^{k-1}$, logo $(\sigma_n)^{(p-1).p^k} = ((\sigma_n)^{(p-1).p^{k-1}})^p = 1$. Fazendo substituição na última congruência obtemos

(3.27) $u^{n^{(p-1).p^k}-1} \equiv 1 \bmod N$

Seja agora r um divisor primo de n. Através do Corolário (3.14) obtemos $u^{r-\sigma_r} \equiv X(r)^{-r.\beta} \bmod rB$, portanto a congruência (3.22) é satisfeita se substituirmos n por r, γ por $X(r)^{-r.\beta}$ e N por rB; então a congruência (3.26) é válida com esses novos valores, ou seja, $u^{r^i-(\sigma_r)^i} \equiv X(r)^{-i.r^i.\beta} \bmod rB$ para todo $i \in Z_+$. Em particular fazendo i = p - 1 obtemos

(3.28) $u^{r^{p-1}-(\sigma_r)^{p-1}} \equiv X(r)^{-(p-1).r^{p-1}.\beta} \bmod rB.$

Numa segunda etapa utilizaremos a condição (2.12): $r^{p-1} = (n^{p-1})^{l_p(r)}$ para algum $l_p(r) \in Z_p$, que nos dá uma igualdade em $1 + pZ_p$, para obter (3.33) que é uma igualdade entre números inteiros envolvendo r e n. Em seguida utilizando (3.33) exibiremos a igualdade (3.34) que relaciona σ_n e σ_r. Essas duas relações são fundamentais para o passo seguinte.

Por (2.12) temos $r^{p-1} = (n^{p-1})^{l_p(r)}$ para algum $l_p(r) \in Z_p$. Seja $l_p(r) = (l_i \bmod p^i)_{i=1}^{\infty}$ com $l_i \in Z$ para todo $i \in Z_+^*$. Escolhamos $m \equiv l_{k-1} \bmod p^{k-1}$ com $m \in Z$. Como analisamos no § 1, Z pode ser visto como um subconjunto de Z_p, assim $m = (m \bmod p^i)_{i=1}^{\infty} \in Z_p$. Recordemos agora que dados $a,b \in Z_p$, $a = (a_i \bmod p^i)_{i=1}^{\infty}$ e $b = (b_i \bmod p^i)_{i=1}^{\infty}$, se $a_k \equiv b_k \bmod p^k$ então $(a_i - b_i) \bmod p^i = 0$ para todo $i \leqslant k$, visto que $a_{i+1} \equiv a_i \bmod p^i$ para todo $i \in Z_+^*$; observemos, pela própria construção de m, que $(m - l_{k-1}) \bmod p^{k-1} = 0$, portanto $(m - l_i) \bmod p^i = 0$ qualquer $i \leqslant k-1$, logo $l_p(r) - m = (z_i \bmod p^i)_{i=1}^{\infty}$ onde $z_i \bmod p^i = 0$ se $1 \leqslant i \leqslant k-1$, e então $l_p(r) - m \in p^k Z_p$, isto é,

(3.29) $l_p(r) - m = p^k.w$ onde $w \in Z_p$

Recorrendo novamente ao § 1, lembremos que se $a \in 1 + pZ_p$ então $a^{Z_p} = \{a^x : x \in Z_p\}$ e $a^{Z_p} = 1 + p^f Z_p$ onde $f = v_p(a - 1)$. Como $(n,p) = 1$, $n^{p-1} \equiv 1 \bmod p$ e então $n^{p-1} = (n^{p-1} \bmod p^i)_{i=1}^{\infty} \in 1 + pZ_p$. De (3.29) temos $p^k.w \in Z_p$ logo $(n^{p-1})^{p^k.w} \in (n^{p-1})^{Z_p}$ de modo que $(n^{p-1})^{p^k.w} \in 1 + p^s Z_p$ onde $s = v_p(n^{p-1} - 1)$. Por outro lado $(n^{p-1})^{p^k} \equiv 1 \bmod p^{k+1}$, então $(n^{p-1})^{p^k} = (n^{(p-1).p^k} \bmod p^i)_{i=1}^{\infty} \in 1 + pZ_p$ e $v_p(n^{(p-1).p^k} - 1) \geqslant k + 1$; assim $(n^{(p-1).p^k})^{Z_p} = 1 + p^d Z_p$ onde $d = v_p(n^{(p-1).p^k} - 1) \geqslant k + 1$. No entanto $(n^{p-1})^{p^k.w} = (n^{(p-1).p^k})^w \in (n^{(p-1).p^k})^{Z_p}$, isto é, $(n^{(p-1).p^k})^w \in 1 + p^d Z_p$, então

(3.30) $v_p(n^{(p-1).p^k.w} - 1) \geqslant d$ com $d = v_p(n^{(p-1).p^k} - 1) \geqslant k + 1$

Sabendo que $r^{p-1} = (n^{p-1})^{l_p(r)}$, encontramos por simples substituição, $r^{p-1} - n^{(p-1).m} = ((n^{p-1})^{l_p(r)-m} - 1).n^{(p-1).m}$ e então

(3.31) $v_p(r^{p-1} - n^{(p-1).m}) = v_p((n^{p-1})^{l_p(r)-m} - 1) + v_p(n^{(p-1).m})$

sendo $v_p(n^{(p-1).m}) = 0$ pois $(p,n) = 1$. Lembrando que $l_p(r) - m = p^k.w$ e utilizando (3.30) a igualdade (3.31) pode ser substituída por

(3.32) $v_p(r^{p-1} - n^{(p-1).m}) = v_p((n^{p-1})^{p^k.w} - 1) \geqslant k + 1$

Então p^{k+1} divide $(r^{p-1} - n^{(p-1).m})$ onde $(r^{p-1} - n^{(p-1).m}) \in Z$, e daí obtemos

(3.33) $n^{(p-1).m} - r^{p-1} = b.p^k$ com $b \in Z$

Desejamos agora provar que

(3.34) $(\sigma_r)^{p-1} = (\sigma_n)^{(p-1).m}$

Para tanto, por definição, $\sigma_r(\zeta_p k) = (\zeta_p k)^r$, então, $(\sigma_r)^{p-1}(\zeta_p k) = (\zeta_p k)^{r^{p-1}}$ e por (3.33) $(\zeta_p k)^{r^{p-1}} = (\zeta_p k)^{n^{(p-1).m}.-b.p^k} = (\zeta_p k)^{n^{(p-1).m}}$; entretanto $\sigma_n(\zeta_p k) = (\zeta_p k)^n$ logo $(\zeta_p k)^{n^{(p-1).m}} = (\sigma_n)^{(p-1).m}(\zeta_p k)$. Com isso $(\sigma_r)^{p-1}(\zeta_p k) = (\sigma_n)^{(p-1).m}(\zeta_p k)$; por outro lado $\sigma_j(\zeta_q) = \zeta_q$ qualquer $\sigma_j \in G$ de modo que os dois automorfismos coincidem nos geradores da extensão $Q(\zeta_p k, \zeta_q)$ de Q e portanto são iguais, isto é, $(\sigma_r)^{p-1} = (\sigma_n)^{(p-1).m}$.

Na terceira etapa construiremos um ideal $R = N + rB$ de modo que todas as congruências válidas módulo N ou módulo rB também serão válidas módulo R. Em particular as congruências (3.26) e (3.28) serão verdadeiras módulo R. Mostraremos então que a divisão de (3.26) por (3.28) pode ser efetuada módulo R. Faremos $i = (p - 1).m$ em (3.26) e explicitaremos o resultado dessa divisão.

Seja $R = N + rB$. R é um ideal de B que contém rB e N o que faz com que as congruências módulo N sejam válidas também módulo R, o mesmo ocorrendo com as congruências módulo rB, portanto, a partir das congruências (3.26) e (3.28) temos

(3.35) $u^{n^i} - (\sigma_n)^i \equiv \eta^{-i.n^i}.\beta \mod R$ para todo $i \in Z_+$

(3.36) $u^{r^{p-1}} - (\sigma_r)^{p-1} \equiv X(r)^{-(p-1).r^{p-1}}.\beta \mod R$

Já provamos anteriormente que T(X) é uma unidade de B, ou equivalentemente, $T(X)^{-1} \in B$, logo $(T(X)^{-1})^x \in B$ para todo

$x \in Z_+$, isto é, $T(X)^{-x} \in B$. Por outro lado $\sigma_x[B] = B$ para todo $\sigma_x \in G$ onde $G = \{\sigma_x : 1 \leqslant x \leqslant p^k;\ x \not\equiv 0 \bmod p\}$ de modo que $\sigma_x(T(X)) \in B$. Dado $\alpha = \sum_{x \in I} n_x.\sigma_x \in Z[G]$, pelas considerações precedentes, $T(X)^{\alpha} = \prod_{\sigma_x \in G} \sigma_x(T(X))^{n_x} \in B$ e pelas mesmas razões $T(X)^{-\alpha} \in B$, logo $T(X)^{\alpha}$ é uma unidade de B qualquer que seja $\alpha \in Z[G]$. Em particular $T(X)^{(r^{p-1}-(\sigma_r)^{p-1}).\beta} = u^{r^{p-1}-(\sigma_r)^{p-1}}$ é uma unidade de B, e portanto é inversível. Claramente $X(r)^{-(p-1).r^{p-1}.\beta}$ também é uma unidade de B visto que $X(r) \in U_p k$. Com $u^{r^{p-1}-(\sigma_r)^{p-1}}$ e $X(r)^{-(p-1).r^{p-1}.\beta}$ inversíveis, podemos dividir (3.35) por (3.36) obtendo

$$(u^{n^i-(\sigma_n)^i})/(u^{r^{p-1}-(\sigma_r)^{p-1}}) \equiv (\eta^{-i.n^i.\beta})/(X(r)^{-(p-1).r^{p-1}.\beta}) \bmod R$$

para todo $i \in Z_+$. Tomando $i = (p-1).m$ encontramos

$$(3.37)\quad u^{n^{(p-1).m}-(\sigma_n)^{(p-1).m}-r^{p-1}+(\sigma_r)^{p-1}} \equiv$$

$$\equiv (\eta^{-(p-1).m.n^{(p-1).m}.\beta})/(X(r)^{-(p-1).r^{p-1}.\beta}) \bmod R$$

No entanto por (3.34): $(\sigma_n)^{(p-1).m} - (\sigma_r)^{p-1} = 0$ o que faz com que o primeiro termo da congruência (3.37) seja igual a $u^{n^{(p-1).m}-r^{p-1}}$. Através de (3.33) obtivemos $n^{(p-1).m} = r^{p-1} + b.p^k$ com $b \in Z$, consequentemente $\eta^{n^{(p-1).m}} = \eta^{r^{p-1}}.(\eta^{p^k})^b = \eta^{r^{p-1}}$ pois $\eta \in U_p k$. Assim o segundo termo da congruência (3.37) se torna $(\eta^{-m}.X(r))^{(p-1).r^{p-1}.\beta}$, portanto (3.37) é equivalente a

$$(3.38)\quad u^{n^{(p-1).m}-r^{p-1}} \equiv (\eta^{-m}.X(r))^{(p-1).r^{p-1}.\beta} \bmod R$$

Na quarta etapa da demonstração, recorreremos a algumas relações que nos permitem reformular (3.38). A nova congruência obtida é (3.40) que nos fornece $\Psi \equiv 1 \bmod R$ onde

$\Psi = (X(r).\eta^{-m})^{(p-1).p^{r-1}.\beta.h}$ é uma raíz p^k-ésima da unidade. Provaremos então que $\Psi \equiv 1 \bmod R$ ocorre se e somente se $X(r) = \eta^m$ e a partir daí chegaremos a $X(r) = \eta^{l_p(r)}$.

Seja $n^{(p-1).p^k} - 1 = h.p^d$ com $d = v_p(n^{(p-1).p^k} - 1)$. De (3.30) e (3.31) obtemos $v_p(n^{(p-1).m} - r^{p-1}) \geqslant v_p(n^{(p-1).p^k} - 1) \geqslant d$; dessa forma p^d divide $(n^{(p-1).m} - r^{p-1})$. Seja $(n^{(p-1).m} - r^{p-1})/p^d = e$; claramente $e \in Z_+$. Se elevarmos (3.38) a $h = (n^{(p-1).p^k} - 1)/p^d$ encontraremos

(3.39) $u^{(n^{(p-1).m} - r^{p-1}).(n^{(p-1).p^k} - 1)/p^d} \equiv$

$(\eta^{-m}.X(r))^{(p-1).r^{p-1}.\beta.h} \bmod R$

Notemos no entanto que $u^{(n^{(p-1).m} - r^{p-1}).(n^{(p-1).p^k} - 1)/p^d} = (u^{n^{(p-1).p^k} - 1})^e$ e por (3.27): $u^{n^{(p-1).p^k} - 1} \equiv 1 \bmod N$ o que resulta em $(u^{n^{(p-1).p^k} - 1})^e \equiv 1 \bmod R$; substituindo esse valor em (3.39) encontramos

(3.40) $1 \equiv (X(r).\eta^{-m})^{(p-1).p^{r-1}.\beta.h} \bmod R$

Observemos agora que $X(r), \eta \in U_{p^k}$ logo $X(r).\eta^{-m} \in U_{p^k}$. Notemos também que $(p-1,p) = 1$; $(r,p) = 1$; $(h,p) = 1$, consequentemente $(p-1).r^{p-1}.h \not\equiv 0 \bmod p$. Por hipótese $\zeta_p^{\beta} \neq 1$ então pela Proposição (3.17) $\sum_{x \in I} x.n_x \not\equiv 0 \bmod p$ de modo que $(p-1).r^{p-1}.h.\sum_{x \in I} x.n_x \not\equiv 0 \bmod p$ e usando novamente a equivalência de (3.17), $\zeta^{(p-1).r^{p-1}.h.\beta} \neq 1$. Constatamos então através da Proposição (3.18) que $\lambda : U_{p^k} \longrightarrow U_{p^k}$ tal que $\lambda(\zeta) = \zeta^{(p-1).r^{p-1}.h.\beta}$ é um automorfismo; dessa forma $(X(r).\eta^{-m})^{(p-1).r^{p-1}.h.\beta} \in U_{p^k}$ pois $X(r).\eta^{-m} \in U_{p^k}$. Aplicando o Le-

ma (3.20) em (3.40) vemos que tal congruência ocorre se e somente se $(X(r).\eta^{-m})^{(p-1)}.r^{p-1}.h.\beta = 1$, contudo λ descrito acima é um automorfismo e então $\lambda(X(r).\eta^{-m}) = (X(r).\eta^{-m})^{(p-1)}.r^{p-1}.h.\beta = 1$ se e somente se $X(r).\eta^{-m} = 1$, isto é, $X(r) = \eta^{m}$. Observemos no entanto por (3.29) que $m = l_p(r) - p^k.w$ então $\eta^m = \eta^{l_p(r)}.(\eta^{p^k})^{-w}$, mas $\eta^{p^k} = 1$ portanto $\eta^m = \eta^{l_p(r)}$ e de $X(r) = \eta^m$ obtemos

(3.41) $X(r) = \eta^{l_p(r)}$

A quinta e última etapa é realmente conclusiva. Nela utilizaremos algumas propriedades dos números inteiros p-ádicos para que a igualdade (3.41) possa ser reformulada até obtermos $X(r) = X(n)^{l_p(r)}$ para todo r divisor primo de n e esse resultado é exatamente a tese do Teorema.

Para $1 \leqslant i \leqslant t$, sejam r_i todos os divisores primos de n. Pela condição (2.12) para cada i existe $l_p(r_i) \in Z_p$ tal que $(r_i)^{p-1} = (n^{p-1})^{l_p(r_i)}$ em $1 + pZ_p$. Já provamos no § 1 que $1 + pZ_p$ mais que um grupo abeliano multiplicativo é um Z_p-módulo; então $(r_i.r_j)^{p-1} = (n^{p-1})^{l_p(r_i)+l_p(r_j)}$ em $1 + pZ_p$ e $((r_i)^{p-1})^{s_i} = (n^{p-1})^{s_i.l_p(r_i)}$ para todo $s_i \in Z_+$. Seja $n = (r_1)^{s_1}.(r_2)^{s_2}.....(r_t)^{s_t} = \prod_{i=1}^{t}(r_i)^{s_i}$, $s_i \in Z_+^*$. Usando os resultados precedentes encontramos $n^{p-1} = (\prod_{i=1}^{t}(r_i)^{s_i})^{p-1} = \prod_{i=1}^{t}(n^{p-1})^{s_i.l_p(r_i)} = (n^{p-1})^{\sum_{i=1}^{t} s_i.l_p(r_i)}$ e essa igualdade só é verdadeira se $\sum_{i=1}^{t} s_i.l_p(r_i) = 1$. Observemos agora que X é um homomorfismo, logo $X(n) = X(\prod_{i=1}^{t}(r_i)^{s_i}) = \prod_{i=1}^{t} X(r_i)^{s_i}$. Notemos no entanto que a igualdade (3.41) é válida para qualquer r divisor primo de n e o η é o mesmo para todos os r, assim, ele-

vando (3.41) a s_i obtemos $X(r_i)^{s_i} = (\eta^{l_p(r_i)})^{s_i}$ para todo $1 \leqslant i \leqslant t$; desse modo $X(n) = \prod_{i=1}^{t} X(r_i)^{s_i} = \prod_{i=1}^{t} (\eta^{l_p(r_i)})^{s_i}$, isto é, $X(n) = \eta^{\sum_{i=1}^{t} s_i \cdot l_p(r_i)}$. Contudo já constatamos que $\sum_{i=1}^{t} s_i \cdot l_p(r_i) = 1$, portanto $X(n) = \eta$. Substituindo-se agora η por $X(n)$ em (3.41) temos $X(r) = X(n)^{l_p(r)}$ para todo r divisor primo de n, e com isso o Teorema está provado. ∎

Nosso próximo passo será desenvolver alguns métodos que podem ser usados para provar que a condição (2.12) é satisfeita. A importância desse passo é que a condição (2.12) aparece como hipótese nos Teoremas (2.11) e (3.21), ambos fundamentais para o teste de primalidade aqui descrito.

Os dois primeiros métodos que serão exibidos são válidos quando o número primo p for diferente de 2.

(3.42) PROPOSIÇÃO: Se $p \geqslant 3$ é um número primo e $n^{p-1} \not\equiv 1 \bmod p^2$ então a condição (2.12) é satisfeita.

PROVA: Pelo Teorema de Fermat, dado $(n,p) = 1$, sabemos que $n^{p-1} \equiv 1 \bmod p$, logo $v_p(n - 1) \geqslant 1$; por outro lado temos por hipótese $n^{p-1} \not\equiv 1 \bmod p^2$ de modo que $p^2 \nmid (n^{p-1} - 1)$, isto é, $v_p(n^{p-1} - 1) < 2$ e então $v_p(n^{p-1} - 1) = 1$. Por (1.14) temos $a^{z_p} = 1 + p^m z_p$ com $m = v_p(a - 1)$, logo $(n^{p-1})^{z_p} = 1 + pz_p$. Novamente pelo Teorema de Fermat temos $r^{p-1} \equiv 1 \bmod p$ visto que $(r,p) = 1$ pois r/n, portanto $r^{p-1} \in 1 + pz_p$ onde $1 + pz_p = (n^{p-1})^{z_p}$. Assim, claramente existe $l_p(r) \in z_p$ tal que $r^{p-1} = (n^{p-1})^{l_p(r)}$ de modo que (2.12) é satisfeita. ∎

Notemos que tal resultado não vale para $p = 2$ pois (1.14) só pode ser usado para $p = 2$ quando $m \geqslant 2$ e no caso da Proposição (3.42) temos $m = 1$.

Se $n^{p-1} \equiv 1 \mod p^2$, recorremos ao seguinte teorema:

(3.43) TEOREMA: Seja $X : F_q^* \longrightarrow U_{p^k}$ tal que $X(g) = \zeta_{p^k}$ com g gerador de F_q^* e assumamos $p \geqslant 3$. Suponhamos que (3.22) é satisfeita com ζ uma raiz p^k-ésima primitiva da unidade. Então p satisfaz (2.12).

PROVA: De modo análogo ao que foi feito na prova do Teorema (3.21) podemos escrever $\zeta = \eta^{-n.\beta}$ com $\eta \in U_{p^k}$; mas aqui, por hipótese, ζ é raíz p^k-ésima primitiva da unidade de modo que η também é raíz p^k-ésima primitiva. Se chamarmos $u = T(X)^{\beta}$ como fizemos no Teorema (3.21) e aplicarmos a congruência (3.26): $u^{n^i} - (\sigma_n)^i = \eta^{-i.n^i.\beta} \mod N$ para $i = p^{k-1}.(p-1)$, obtemos

$$(3.44)\quad u^{n^{p^{k-1}.(p-1)}} - (\sigma_n)^{p^{k-1}.(p-1)} \equiv \eta^{-(p-1).p^{k-1}.n^{(p-1).p^{k-1}}.\beta} \mod N$$

Notemos que $\sigma_n \in G$ onde G é o grupo de Galois de $Q(\zeta_{p^k}, \zeta_q)$ sobre $Q(\zeta_q)$ e já observamos anteriormente que $G \simeq (Z/p^kZ)^*$ cuja ordem é $(p-1).p^{k-1}$, assim $(\sigma_n)^{(p-1).p^{k-1}} = 1$. Notemos também que $n^{(p-1).p^{k-1}} \equiv 1 \mod p^k$ de onde encontramos $n^{(p-1).p^{k-1}} = 1 + p^k.w$ com $w \in Z$; assim $-(p-1).p^{k-1}.n^{(p-1).p^{k-1}}.\beta = -p^k.(1+p^k.w).\beta + p^{k-1}.(1+p^k.w).\beta$ de modo que $\eta^{-(p-1).p^{k-1}.n^{(p-1).p^{k-1}}.\beta} = (\eta^{p^k})^{-(1+p^k.w).\beta}.\eta^{p^{k-1}.\beta}.(\eta^{p^k.w})^{p^{k-1}.\beta} = \eta^{p^{k-1}.\beta}$ pois $\eta^{p^k} = 1$.

Se substituirmos em (3.44) os novos valores encontrados obteremos

$$(3.45)\quad u^{n^{(p-1).p^{k-1}} - 1} \equiv \eta^{p^{k-1}.\beta} \bmod N$$

Seja r divisor primo de n. Recorrendo à prova do Teorema (3.21) notamos que podemos substituir na congruência acima n por r, η por X(r) e N por rB obtendo

$$(3.46)\quad u^{r^{(p-1).p^{k-1}} - 1} \equiv X(r)^{p^{k-1}.\beta} \bmod rB$$

Se tomarmos R = nB + N, as congruências (3.45) e (3.46) continuam válidas módulo R.

Já provamos anteriormente que $u = T(X)^{\beta} \in B^*$ de modo que u mod R $\in (B/R)^*$. Seja $\hat{w}$ a ordem de u mod R em $(B/R)^*$, isto é, $u^{\hat{w}} \equiv 1 \bmod R$.

η é raíz p^k-ésima primitiva da unidade, logo $\eta^{p^{k-1}}$ é raíz p-ésima primitiva da unidade e então $\eta^{p^{k-1}} \neq 1$. A condição (3.22) é satisfeita por hipótese, isto é, β satisfaz $(\zeta_p)^{\beta} \neq 1$ e obtemos $(\eta^{p^{k-1}})^{\beta} \neq 1$ o que implica em $(\eta^{p^{k-1}})^{\beta} \not\equiv 1 \bmod R$ pois o Lema (3.20) afirma que se $\zeta \in U_{p^k}$ e $\zeta \equiv 1 \bmod R$ então $\zeta = 1$. Lembrando que as congruências módulo N também são válidas módulo R constatamos a partir de (3.45) que $u^{n^{(p-1).p^{k-1}} - 1} \not\equiv 1 \bmod R$. No entanto $(\eta^{p^{k-1}.\beta})^p = (\eta^{p^k})^{\beta} = 1$ de modo que $u^{p.(n^{(p-1).p^{k-1}} - 1)} \equiv 1 \bmod R$, portanto $\hat{w}/p.(n^{(p-1).p^{k-1}} - 1)$; então $p.(n^{(p-1).p^{k-1}} - 1) = \hat{w}.s$ onde $s \in \mathbb{Z}_+$ e (s,p) = 1 visto que $\hat{w} \not| (n^{(p-1).p^{k-1}} - 1)$. Encontramos $n^{(p-1).p^{k-1}} - 1 = (\hat{w}.s)/p$, logo $v_p(n^{(p-1).p^{k-1}} - 1) = v_p(\hat{w}) + v_p(s) - v_p(p) = v_p(\hat{w}) - 1$ pois

$v_p(s) = 0$.

Passemos agora a analisar o número primo r:

$X(r) \in U_p^k$, logo $(X(r)^{p^{k-1}}.\beta)^p = 1$ e então elevando (3.46) a potência p obtemos $u^{p.(r^{(p-1).p^{k-1}} - 1)} \equiv 1 \bmod rB$ de modo que $u^{p.(r^{(p-1).p^{k-1}} - 1)} \equiv 1 \bmod R$, logo $\hat{w}/p.(r^{(p-1).p^{k-1}} - 1)$ e daí $v_p(\hat{w}) \leqslant v_p(p) + v_p(r^{(p-1).p^{k-1}} - 1)$. Substituindo $v_p(\hat{w})$ por $v_p(n^{(p-1).p^{k-1}} - 1) + 1$ encontramos

(3.47) $v_p(n^{(p-1).p^{k-1}} - 1) \leqslant v_p(r^{(p-1).p^{k-1}} - 1)$

Seja $a = v_p(r^{(p-1).p^{k-1}} - 1)$ e $b = v_p(n^{(p-1).p^{k-1}} - 1)$.

Claramente $a \geqslant b$. Por (1.14) temos $(n^{(p-1).p^{k-1}})^{Z_p} = 1 + p^b Z_p$ e $1 + p^b Z_p \supset 1 + p^a Z_p$, logo $r^{(p-1).p^{k-1}} \in (n^{(p-1).p^{k-1}})^{Z_p}$, portanto existe $t \in Z_p$ tal que $r^{(p-1).p^{k-1}} = (n^{(p-1).p^{k-1}})^t \in Z_p^*$. Notamos então que $(n^{(p-1).t/r^{p-1}})^{p^{k-1}} = 1$ e $1 \in Z_p^*$; pelo isomorfismo (1.26) observamos que Z_p^* não possui elemento de ordem p, então $(n^{(p-1).t/r^{p-1}})^{p^{k-1}} = 1$ se e somente se $n^{(p-1).t/r^{p-1}} = 1$, ou seja, $r^{p-1} = n^{(p-1).t}$ e provamos assim que (2.12) é satisfeita. ∎

(3.48) Observamos aqui que a prova feita no Teorema (3.43) para obter a desigualdade (3.47) também é válida para $p = 2$ pois embora o Teorema tenha como hipótese $p \geqslant 3$, esse fato só é utilizado depois de obtermos (3.47); com isso a desigualdade (3.47) é válida para qualquer primo p, desde que a condição (3.22) seja satisfeita.

Os próximos resultados deste parágrafo abordarão o nú-

mero primo p = 2.

Definiremos a seguir resíduo quadrático módulo p e Símbolo de Legendre; daremos alguns resultados relacionados a eles que serão necessários no Lema (3.52) e na Proposição (3.56).

Para todo b tal que (b,m) = 1, b é chamado um resíduo quadrático módulo m se a congruência $x^2 \equiv b \bmod m$ tem solução. Se ela não tem solução, então b é chamado resíduo não quadrático módulo m.

(3.49) Se p é um número primo ímpar e (b,p) = 1, o Símbolo de Legendre $\left(\frac{b}{p}\right)$ é definido igual a 1 se b é um resíduo quadrático e -1 se b é um resíduo não quadrático módulo p.

(3.50) PROPOSIÇÃO: Se p é um número primo ímpar e $a \in \mathbb{Z} - p\mathbb{Z}$ então $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$.

PROVA: Algebraic Theory of Numbers - Pierre Samuel - 5.5 Proposition 1

ou

An Introduction to the Theory of Numbers - Ivan Niven; Herbert Zuckerman - Theorem 3.1

(3.51) PROPOSIÇÃO:
$$\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ se } p \equiv \pm 1 \bmod 8 \\ -1 \text{ se } p \equiv \pm 3 \bmod 8 \end{cases}$$

PROVA: Introdução a Algebra e Aritmética - T. M. Viswanathan

(3.52) LEMA: Seja $a \in \mathbb{Z}$ e suponhamos que $a^{(n-1)/2} \equiv -1 \bmod n$. Então para todo r divisor primo de n nós temos $v_2(r-1) \geqslant v_2(n-1)$. A igualdade ocorre se e somente se $\left(\frac{a}{r}\right) = -1$.

PROVA: Temos por hipótese $a^{(n-1)/2} \equiv -1 \bmod n$, logo $a^{(n-1)/2} \equiv -1 \bmod r$ visto que r é divisor de n, portanto r não divide a e assim a mod r $\in (\mathbb{Z}/r\mathbb{Z})^*$. Seja w a ordem de a mod r no grupo $(\mathbb{Z}/r\mathbb{Z})^*$, isto é, $a^w \equiv 1 \bmod r$; como a ordem de $(\mathbb{Z}/r\mathbb{Z})^*$ é r - 1 concluímos que w/(r-1) de modo que

(3.53) $v_2(w) \leqslant v_2(r-1)$

Notamos também que $w \not| (n-1)/2$ pois $a^{(n-1)/2} \equiv -1 \bmod r$ contudo $a^{n-1} \equiv 1 \bmod r$, logo w/(n-1). Seja $n-1 = w.b.2^i$ onde $b,i \in \mathbb{Z}_+$, (b,2) = 1. Claramente i = 0 pois se i > 0 teríamos $(n-1)/2 = w.b.2^{i-1}$ e então $w \not| (n-1)/2$ e isso não ocorre; assim $n-1 = w.b$ e $v_2(n-1) = v_2(w) + v_2(b) = v_2(w)$ pois por hipótese (b,2) = 1. Substituindo $v_2(n-1)$ por $v_2(w)$ em (3.53) obtemos a igualdade desejada, ou seja, $v_2(n-1) \leqslant v_2(r-1)$.

Para verificarmos quando ocorre a igualdade notemos que $w \not| ((r-1)/2)$ se e somente se $a^{(r-1)/2} \equiv -1 \bmod r$ e utilizando (3.50) a congruência ocorre se e somente se $\left(\frac{a}{r}\right) = -1$; assim $r-1 = w.t$ com (t,2) = 1, de modo que $v_2(r-1) = v_2(w) + v_2(t) = v_2(w)$ e então encontramos $v_2(n-1) = v_2(w) = v_2(r-1)$.

A seguir enunciaremos e provaremos alguns resultados para os quais a condição (2.12) é satisfeita.

(3.54) PROPOSIÇÃO: Suponhamos que $n \equiv 1 \bmod 4$ e que existe $a \in \mathbb{Z}$ para o qual $a^{(n-1)/2} \equiv -1 \bmod n$. Então a condição (2.12) é satisfeita para $p = 2$.

PROVA: Seja r um divisor primo de n. Por hipótese $a^{(n-1)/2} \equiv -1 \bmod n$, de modo que o Lema (3.52) pode ser aplicado e dele obtemos $v_2(r-1) \geqslant v_2(n-1)$. Como $n \equiv 1 \bmod 2^2$ observamos que $v_2(n-1) \geqslant 2$. Recorrendo a (1.14) lembremos que $d^{\mathbb{Z}_2} = 1 + 2^m\mathbb{Z}_2$ com $m = v_2(d-1)$ desde que $m \geqslant 2$. Assim temos $n^{\mathbb{Z}_2} = 1 + 2^m\mathbb{Z}_2$ com $m = v_2(n-1) \geqslant 2$ e por sua vez $v_2(r-1) \geqslant v_2(n-1) \geqslant m$, então $r \in 1 + 2^m\mathbb{Z}_2$ com $1 + 2^m\mathbb{Z}_2 = n^{\mathbb{Z}_2}$, portanto existe $l_2(r) \in \mathbb{Z}_2$ tal que $r = n^{l_2(r)}$ e esta é a igualdade desejada visto que neste caso $p-1 = 1$. ∎

Antes de enunciar a próxima proposição provaremos uma igualdade bastante simples que será utilizada a seguir.

(3.55) $n^{\mathbb{Z}_2} = n^{2\mathbb{Z}_2} \cup n^{1+2\mathbb{Z}_2}$

Claramente $n^{\mathbb{Z}_2} \supset n^{2\mathbb{Z}_2} \cup n^{1+2\mathbb{Z}_2}$. Para provar a outra inclusão lembremos que $\mathbb{Z}_p^* = \mathbb{Z}_p - p\mathbb{Z}_p$, então $\mathbb{Z}_2 = \mathbb{Z}_2^* \cup 2\mathbb{Z}_2$. Por (1.27) temos $\mathbb{Z}_2^* = 1 + 2\mathbb{Z}_2$ de modo que $\mathbb{Z}_2 = (1 + 2\mathbb{Z}_2) \cup 2\mathbb{Z}_2$; assim dado $z \in \mathbb{Z}_2$, ou $z \in (1 + 2\mathbb{Z}_2)$ ou $z \in 2\mathbb{Z}_2$, logo $n^z \in n^{1+2\mathbb{Z}_2}$ ou $n^z \in n^{2\mathbb{Z}_2}$, portanto, qualquer que seja $n^z \in n^{\mathbb{Z}_2}$ teremos $n^z \in n^{2\mathbb{Z}_2} \cup n^{1+2\mathbb{Z}_2}$ e isso implica em $n^{\mathbb{Z}_2} \subset n^{2\mathbb{Z}_2} \cup n^{1+2\mathbb{Z}_2}$. Combinando as duas inclusões obtemos a igualdade (3.55).

(3.56) PROPOSIÇÃO: Suponhamos que $n \equiv 3 \bmod 8$ e que

$2^{(n-1)/2} \equiv -1 \bmod n$. Então a condição (2.12) é satisfeita para $p = 2$.

PROVA: Por hipótese $n \equiv 3 \bmod 8$ o que implica em $v_2(n-1) = 1$. Seja r divisor primo ímpar de n, $r \equiv 1, 3, 5$ ou $7 \bmod 8$. Se $r \equiv 1$ ou $5 \bmod 8$, $v_2(r-1) \geqslant 2 > v_2(n-1)$ e pelo Lema (3.52) $\left(\frac{2}{r}\right) = 1$; mas, de acordo com (3.51) se $r \equiv 5 \bmod 8$ temos $\left(\frac{2}{r}\right) = -1$. Então se $n \equiv 3 \bmod 8$ e $2^{(n-1)/2} \equiv -1 \bmod n$, n não possui divisor primo r com $r \equiv 5 \bmod 8$. Se $r \equiv 3$ ou $7 \bmod 8$, $v_2(r-1) = 1 = v_2(n-1)$ e pelo Lema (3.52) $\left(\frac{2}{r}\right) = -1$. Novamente recorrendo a (3.51) observamos que para $r \equiv 7 \bmod 8$ temos $\left(\frac{2}{r}\right) = 1$ de modo que n também não possui divisor primo r com $r \equiv 7 \bmod 8$. Concluímos então que existem apenas duas possibilidades para r: $r \equiv 1 \bmod 8$ ou $r \equiv 3 \bmod 8$.

Notemos agora que a igualdade (1.14) não pode ser utilizada aqui visto que $v_2(n-1) = 1 < 2$ e assim não podemos afirmar que $n^{Z_2} = 1 + 2Z_2$, porém sabemos que $n = 3 + 8.b$ com $b \in Z$, portanto $n^2 = 1 + 8.(1 + 6.b + 8.b^2)$ e $v_2(n^2 - 1) = 3$. Agora (1.14) pode ser aplicada para $a = n^2$ e daí obtemos $n^{2Z_2} = 1 + 2^3 Z_2$.

Para $r \equiv 1 \bmod 8$ temos $v_2(r-1) \geqslant 3$ de modo que $r \in n^{2Z_2}$ e por (3.55) $r \in n^{Z_2}$, logo existe $t \in Z_2$ tal que $r = n^t$.

Para $r \equiv 3 \bmod 8$, $r \equiv n \bmod 8$ e então $r.n^{-1} \equiv 1 \bmod 8$, portanto $v_2(r.n^{-1} - 1) \geqslant 3$, logo $r.n^{-1} \in n^{2Z_2}$ de modo que existe $z \in Z_2$ tal que $r.n^{-1} = n^{2.z}$ e daí $r = n^{1+2.z} \in n^{1+2Z_2}$ mas por (3.55) $n^{1+2Z_2} \subset n^{Z_2}$ o que implica em $r \in n^{Z_2}$ e então existe $t \in Z_2$ tal que $r = n^t$.

Portanto se r é um divisor primo ímpar de n com

$n \equiv 3 \bmod 8$ e $2^{(n-1)/2} \equiv -1 \bmod 8$ então a condição (2.12) é satisfeita para $p = 2$. ∎

Notemos que de certa forma as Proposições (3.54) e (3.56) fornecem critérios para analisar os números inteiros n côngruos a 1, 3 ou 5 módulo 8; falta no entanto um critério para $n \equiv 7 \bmod 8$ que será desenvolvido posteriormente.

Enunciaremos agora uma proposição relativa a números primos e a seguir provaremos um teorema a respeito da validade da condição (2.12).

(3.57) PROPOSIÇÃO: Suponhamos que n é um número primo e que (3.22) é satisfeita para uma raiz 2^k-ésima primitiva da unidade, onde $k \geqslant 2$. Se 2^k divide $(q-1)$ então $q^{(n-1)/2} \equiv -1 \bmod n$.

PROVA: Pelo Corolário (3.14) se n é primo então $T(X)^{(n-\sigma_n)\cdot\beta} \equiv X(n)^{-n\cdot\beta} \bmod N$ para todo $\beta \in Z[G]$ e todo ideal N de $B = Z[\zeta_2 k, \zeta_q]\left[\frac{1}{q}\right]$ com $n \in N$; em particular o Corolário é válido para β e N da condição (3.22). Por outro lado a condição (3.22) é satisfeita aqui para uma raiz 2^k-ésima primitiva da unidade ζ, ou seja, $T(X)^{(n-\sigma_n)\cdot\beta} \equiv \zeta \bmod N$. Combinando essa congruência com a anterior obtemos $\zeta \equiv X(n)^{n\cdot\beta} \bmod N$. Lembremos agora que X(n) é uma raiz 2^k-ésima da unidade e para esse β em particular (β satisfaz (3.15)) a função $\lambda : \eta \longrightarrow \eta^{\beta}$ é um automorfismo de $U_2 k$; como $(p,n) = 1$, $\varphi : \eta \longrightarrow \eta^{-n\cdot\beta}$ também é um automorfismo de $U_2 k$. Assim $X(n)^{-n\cdot\beta}$ é uma raiz 2^k-ésima da unidade e seu inverso também é, de modo que $\zeta . X(n)^{n\cdot\beta}$ é raiz 2^k-ésima da unidade. De

$\zeta \equiv X(n)^{-n.\beta} \bmod N$ obtemos $\zeta.X(n)^{n.\beta} \equiv 1 \bmod N$. Se $R = rB + N$, claramente $\zeta.X(n)^{n.\beta} \equiv 1 \bmod R$ e pelo Lema (3.20) essa última congruência implica em $\zeta.X(n)^{n.\beta} = 1$, logo $\zeta = X(n)^{-n.\beta}$, consequentemente $X(n)^{-n.\beta}$ é uma raiz 2^k-ésima primitiva; mas $\varphi(\eta) = \eta^{-n.\beta}$ é um automorfismo e esse fato faz de $X(n)$ uma raiz 2^k-ésima primitiva da unidade. Verificamos então que $X(n)^{2^{k-1}} \neq 1$ mas $X(n)^{2^{k-1}}$ é uma raiz 2-ésima da unidade, portanto $X(n)^{2^{k-1}} \neq 1$ implica em $X(n)^{2^{k-1}} = -1$. Seja $\Psi = X^{2^{k-1}}$, então $\Psi(n) = -1$. Claramente $\Psi : F_q^* \longrightarrow \{-1, 1\}$ é uma função caracter de ordem 2, logo $\Psi = \Psi^{-1}$. Por (3.9) temos $T(\Psi).T(\Psi^{-1}) = \Psi(-1).q$, portanto $T(\Psi)^2 = \Psi(-1).q$. Como $k \geqslant 2$ temos $\Psi(-1) = X^{2^{k-1}}(-1) = (X(-1)^2)^{2^{k-2}}$ mas $X(-1)^2 = X(1) = 1$ então $\Psi(-1) = 1$; desse modo

(3.58) $\quad T(\Psi)^2 = q$

Pelo Lema (3.13) se n é primo temos

(3.59) $\quad T(\Psi)^{n-\sigma_n} \equiv \Psi(n)^{-n} \bmod nB$

Recordando que $\sigma_n(\zeta_{2^k}) = (\zeta_{2^k})^n$, $\sigma_n(\zeta_q) = \zeta_q$, $T(\Psi) = \sum_{x=1}^{q-1} \Psi(x).(\zeta_q)^x$, $\Psi(x) = \pm 1$ notamos que $T(\Psi)^{\sigma_n} = \sigma_n(T(\Psi)) = T(\Psi)$. Assim, substituindo em (3.59) $T(\Psi)^{\sigma_n}$ por $T(\Psi)$ e $\Psi(n)$ por -1 obtemos $T(\Psi)^{n-1} \equiv -1 \bmod nB$, ou equivalentemente $(T(\Psi)^2)^{(n-1)/2} \equiv -1 \bmod nB$; utilizando (3.58) encontramos $q^{(n-1)/2} \equiv -1 \bmod nB$, isto é, $q^{(n-1)/2} + 1 \equiv 0 \bmod nB$. Observemos agora que $q^{(n-1)/2} + 1 \in Z$ e então $q^{(n-1)/2} + 1 \in Z \cap nB$. No entanto $nB \subset N$ e por hipótese N satisfaz (3.16): $N \cap Z = nZ$ de modo que $nB \cap Z \subset N \cap Z$ com $N \cap Z = nZ$, portanto $q^{(n-1)/2} + 1 \in nZ$, isto é, $q^{(n-1)/2} \equiv -1 \bmod n$. ∎

(3.60) TEOREMA: Seja X uma função caracter módulo q de ordem 2^k, com $k \geqslant 2$. Suponha que (3.22) é satisfeita com uma raiz 2^k-ésima primitiva da unidade ζ. Suponhamos também que $q^{(n-1)/2} \equiv -1 \bmod n$. Então a condição (2.12) é satisfeita para p = 2.

PROVA: Se $n \equiv 1 \bmod 4$ e $q^{(n-1)/2} \equiv -1 \bmod n$ podemos utilizar a Proposição (3.54) de modo que a condição (2.12) é satisfeita para p = 2, logo assumiremos a partir daqui $n \equiv 3 \bmod 4$.

O teorema enunciado acima consiste em provar que existe um $t \in \mathbb{Z}_2$ tal que $r = n^t$ no grupo $1 + 2\mathbb{Z}_2$. Devido a extensão da demonstração, ela será dividida em quatro etapas.

Na primeira etapa utilizaremos valorizações 2-ádicas para concluirmos que existe $t \in \mathbb{Z}_2$ tal que $r = \pm n^t$. O restante da prova visará conseguir argumentos para tornar inviável a possibilidade de $r = -n^t$.

Como vimos em (3.48), (3.47) é válida para p = 2; temos então

$$(3.61)\quad v_2(r^{2^{k-1}} - 1) \geqslant v_2(n^{2^{k-1}} - 1)$$

Como no Teorema (3.43) a igualdade ocorre se e somente se $X(r)^{p^{k-1}} \neq 1$ (teremos a igualdade aqui se e somente se $X(r)^{2^{k-1}} \neq 1$). Se definirmos $\Psi = X^{2^{k-1}}$, a igualdade ocorre quando $\Psi(r) \neq 1$, mas claramente a imagem da função $\Psi : F_q^* \longrightarrow \langle \zeta_{2^k} \rangle$ é igual a $\{1, -1\}$, então se $\Psi(r) \neq 1$ teremos $\Psi(r) = -1$; portanto a partir de (3.61) obtemos

$$(3.62)\quad v_2(r^{2^{k-1}} - 1) = v_2(n^{2^{k-1}} - 1) \text{ se e somente se } \Psi(r) = -1$$

Dando prosseguimento, lembremos que $k \geqslant 2$. Desde que

$n \equiv 3 \bmod 4$ temos $n = 3 + 4.x$ com $x \in Z$, assim $n^2 = 9 + 8.3.x + 16.x^2 = 1 + 8.(1 + 3.x + 2.x^2)$, portanto $v_2(n^2 - 1) \geqslant 3$. Se $k = 2$ obtemos $n^{2^{k-1}} - 1 = n^2 - 1$, logo $v_2(n^{2^{k-1}} - 1) \geqslant 3$. Se $k > 2$ obtemos $n^{2^{k-1}} - 1 = (n^2 - 1).\prod_{i=1}^{k-2}(n^{2^{k-1-i}} + 1)$ e $v_2(n^{2^{k-1}} - 1) = v_2(n^2 - 1) + \sum_{i=1}^{k-2} v_2(n^{2^{k-1-i}} + 1) \geqslant 3$. De $m = v_2(n^{2^{k-1}} - 1) \geqslant 3$ concluímos por (1.14) que $(n^{2^{k-1}})^{Z_2} = 1 + 2^m Z_2$ e a partir de (3.61) constatamos que $r^{2^{k-1}} \in (n^{2^{k-1}})^{Z_2}$; assim existe $t \in Z_2$ tal que $r^{2^{k-1}} = n^{2^{k-1}.t}$ e então $(n^t/r)^{2^{k-1}} = 1 \in Z_2^*$. No entanto por (1.27): $Z_2^* \cong \{1, -1\} \times (1 + 4Z_2)$ de modo que os únicos elementos de ordem finita de Z_2^* são 1 e -1 que por sua vez são as únicas raízes 2^k-ésimas da unidade que pertencem a Z_2^*, portanto $n^t/r = \pm 1$, ou seja,

(3.63) $r = \pm n^t$

Iniciaremos agora a segunda etapa da demonstração. Recorreremos a algumas propriedades de números inteiros 2-ádicos para definir números inteiros 2-ádicos pares e ímpares; a partir disso provaremos que $\Psi(r) = X^{2^{k-1}}(r) = -1$ se e somente se o t encontrado na primeira etapa for ímpar; daí concluiremos que $\Psi(r) = (-1)^t$. Recordando, x pertencente a $Z_2 = Z_2^* \cup 2Z_2$ é da forma $x = (x_i \bmod 2^i)_{i=1}^{\infty}$ com $x_i \in Z$, $x_i \bmod 2^i \in Z/2^iZ$ e $x_{i+1} \equiv x_i \bmod 2^i$, de modo que $x_1 \equiv 0$ ou $1 \bmod 2$. Diremos que x é par se x_1 for par, ou equivalentemente, $x_1 \equiv 0 \bmod 2$; x será ímpar se x_1 for ímpar, ou equivalentemente $x_1 \equiv 1 \bmod 2$. Notemos que

se x é par, $x \in 2\mathbb{Z}_2$ e se x é ímpar então $x \in \mathbb{Z}_2^*$. Como fizemos em (1.4), seja $E = \{1, -1\}$ e $x = (x_i \bmod 2^i)_{i=1}^{\infty} \in \mathbb{Z}_2$. Dado $\zeta \in E$ definimos anteriormente $\zeta^x = \zeta^{x_m}$ para m suficientemente grande. Nesse caso $\zeta = \pm 1$, portanto basta tomarmos m = 1, ou seja, $\zeta^x = \zeta^{x_1}$. Assim, se $t = (t_i \bmod 2^i)_{i=1}^{\infty} \in \mathbb{Z}_2$ com $t_i \in \mathbb{Z}$, teremos

$$(3.64) \quad \begin{cases} (-1)^t = (-1)^{t_1} = -1 & \text{se t for ímpar} \\ (-1)^t = (-1)^{t_1} = 1 & \text{se t for par} \end{cases}$$

A partir dessas observações provaremos a seguir que:

(3.65) $\Psi(r) = -1$ se e somente se t é ímpar

Por (3.63) temos $r = \pm n^t$, portanto $r^2 = n^{2.t}$. O teorema tem como hipótese $k \geqslant 2$, logo $r^{2^{k-1}} = (r^2)^{2^{k-2}} = (n^{2.t})^{2^{k-2}} = n^{2^{k-1}.t}$. Dado $\Psi(r) = -1$ temos por (3.62): $v_2(r^{2^{k-1}} - 1) = v_2(n^{2^{k-1}} - 1)$ e substituindo $r^{2^{k-1}}$ por $n^{2^{k-1}.t}$ encontramos $v_2(n^{2^{k-1}.t} - 1) = v_2(n^{2^{k-1}} - 1) \geqslant 3$. Dessa igualdade notamos que $(n^{2^{k-1}})^{\mathbb{Z}_2} = (n^{2^{k-1}.t})^{\mathbb{Z}_2}$ de modo que $n^{2^{k-1}} \in (n^{2^{k-1}.t})^{\mathbb{Z}_2}$; assim existe $t' \in \mathbb{Z}_2$ tal que $n^{2^{k-1}} = n^{2^{k-1}.t.t'}$ e já vimos anteriormente que essa igualdade ocorre se e somente se $t.t' = 1$, portanto $t \in \mathbb{Z}_2^*$, isto é, t é ímpar. Recíprocamente se t é ímpar, $t \in \mathbb{Z}_2^*$ e existe $t' \in \mathbb{Z}_2$ tal que $t.t' = 1$ de modo que $n^{2^{k-1}} = (n^{2^{k-1}.t})^{t'} \in (n^{2^{k-1}.t})^{\mathbb{Z}_2}$; daí obtemos $v_2(n^{2^{k-1}} - 1) \geqslant v_2(n^{2^{k-1}.t} - 1) = v_2(r^{2^{k-1}} - 1)$, mas por (3.61): $v_2(n^{2^{k-1}} - 1) \leqslant v_2(r^{2^{k-1}} - 1)$ e então temos a igualdade, o que implica por (3.62) em $\Psi(r) = -1$ e concluímos a prova de (3.65). Do fato de $\Psi(r) = -1$ se e somente se t é ímpar é fácil concluir que

(3.66) $\Psi(r) = (-1)^t$

Nesta terceira etapa trabalharemos com Somas de Gauss e resíduos quadráticos módulo r e q para obter $\Psi(r) = \left(\frac{r}{q}\right) = \left(\frac{q}{r}\right)$. $\Psi : F_q^* \longrightarrow \{1, -1\}$ é uma função quadrática. Sabemos que $F_q^* = (F_q^*)^2 \cup g.(F_q^*)^2$ onde g não é um quadrado módulo q e $\Psi(g) = -1$, logo $\Psi(x) = 1$ se $x \in (F_q^*)^2$ e $\Psi(x) = -1$ se $x \notin (F_q^*)^2$. Assim, de acordo com a definição de resíduo quadrático módulo q temos $\Psi(x) = \left(\frac{x}{q}\right)$ para $x \in Z$, $(x,q) = 1$, portanto

(3.67) $\Psi(r) = \left(\frac{r}{q}\right)$

Recorrendo agora a Soma de Gauss, em (3.9) temos $T(\Psi)^2 = \Psi(-1).q$, mas nesse caso $\Psi(-1) = 1$ pois $k \geqslant 2$ implica em $\Psi(-1) = (X(-1)^2)^{2^{k-2}}$ e $X(-1)^2 = X(1) = 1$, portanto

(3.68) $T(\Psi)^2 = q$

Como r é um número primo o Lema (3.13) pode ser utilizado substituindo-se n por r e X por Ψ; temos assim $T(\Psi)^{r-\sigma_r} \equiv \Psi(r)^{-r} \bmod rB$ com $B = Z[\zeta_2 k, \zeta_q]\left[\frac{1}{q}\right]$. Lembremos que $T(\Psi) = \sum_{x=1}^{q-1} \Psi(x).(\zeta_q)^x$, $\sigma_r(\zeta_2 k) = (\zeta_2 k)^r$ e $\sigma_r(\zeta_q) = \zeta_q$. Como $\Psi(x)^r = (\pm 1)^r = \Psi(x)$ pois r é ímpar, temos $\sigma_r(T(\Psi)) = T(\Psi)$. Assim a última congruência obtida é equivalente a

(3.69) $T(\Psi)^{r-1} \equiv \Psi(r) \bmod rB$. Vemos de um lado por (3.68) que $(T(\Psi)^{(r-1)/2})^2 = (T(\Psi)^2)^{(r-1)/2} = q^{(r-1)/2}$ e de outro lado por (3.67) $\Psi(r) = \left(\frac{r}{q}\right)$, logo a congruência (3.69) pode ser substituída por $q^{(r-1)/2} \equiv \left(\frac{r}{q}\right) \bmod rB$, mas $\left(\frac{r}{q}\right) \in Z$ e $q^{(r-1)/2} \in Z$ de modo que $q^{(r-1)/2} - \left(\frac{r}{q}\right) \in rB \cap Z = rZ$, logo $q^{(r-1)/2} \equiv \left(\frac{r}{q}\right) \bmod r$. No entanto, por definição, $q^{(r-1)/2} \equiv \left(\frac{q}{r}\right) \bmod r$, portanto $\left(\frac{r}{q}\right) \equiv \left(\frac{q}{r}\right) \bmod r$, mas $\left(\frac{r}{q}\right) = \pm 1$ e $\left(\frac{q}{r}\right) = \pm 1$, então $\left(\frac{r}{q}\right) = \left(\frac{q}{r}\right)$ ou $\left(\frac{r}{q}\right) = -\left(\frac{q}{r}\right)$. Para

provar que são iguais, suponhamos que $\left(\frac{r}{q}\right) = -\left(\frac{q}{r}\right)$; teremos então $2 \equiv 0 \bmod r$ o que é absurdo pois r é um número primo ímpar, portanto $\left(\frac{r}{q}\right) = \left(\frac{q}{r}\right)$ e então por (3.67) temos $\Psi(r) = \left(\frac{r}{q}\right) = \left(\frac{q}{r}\right)$.

Finalmente usando a hipótese adicional $q^{(n-1)/2} \equiv -1 \bmod n$ provaremos que $r \equiv \Psi(r) \bmod 4$ e daí concluiremos que $r = n^t$.

Utilizaremos agora a hipótese $q^{(n-1)/2} \equiv -1 \bmod n$; ela nos dá condições para aplicarmos o Lema (3.52) de onde obtemos

(3.70) $v_2(r - 1) \geqslant v_2(n - 1)$

A igualdade ocorre se e somente se $\Psi(r) = -1$ pois $\left(\frac{q}{r}\right) = \Psi(r)$.

Vamos agora analisar o que acontece quando $\Psi(r) = 1$ ou -1. Se $\Psi(r) = -1$ temos igualdade em (3.61) e em (3.70). Se $\Psi(r) = 1$ temos desigualdade estrita em (3.61) e (3.70). Temos por hipótese $n \equiv 3 \bmod 4$ o que implica em $n - 1 = 2.(1 + 2.x)$ com $x \in Z$, portanto $v_2(n - 1) = 1$. Assim, se $\Psi(r) = -1$ teremos $v_2(r - 1) = v_2(n - 1) = 1$, de onde obtemos $r \equiv 1 \bmod 2$ e $r \not\equiv 1 \bmod 4$, logo $r - 1 = 2.k$ com k ímpar, ou equivalentemente, $r - 1 + 2 = 2.k + 2$, ou seja, $r + 1 = 2.(k + 1)$. Como k é ímpar $(k + 1)$ é par e então $r + 1 = 4.z$ com $z \in Z$ e obtemos $r \equiv -1 \bmod 4$, portanto $r \equiv \Psi(r) \bmod 4$.

Se $\Psi(r) = 1$ teremos $v_2(r - 1) > v_2(n - 1) = 1$ o que implica em $r \equiv 1 \bmod 4$, portanto $r \equiv \Psi(r) \bmod 4$. Dado $n \in 1 + pZ_p$ e $x \in Z_p$ com $x = (x_i \bmod p^i)_{i=1}^{\infty}$ e $x_i \in Z$, já verificamos anteriormente que $n^x = n^{x_i}$ para i suficientemente grande. Utilizando então (3.66) e $n \equiv -1 \bmod 4$, $r \equiv \Psi(r) \equiv (-1)^t \equiv n^t \bmod 4$, isto é,

$r \equiv n^t \bmod 4$. Mas $r = \pm n^t$. Se supusermos $r = -n^t$ teremos $r \equiv -r \bmod 4$, ou seja, $2.r \equiv 0 \bmod 4$ e isso implica em $2.r = 4.k$ com $k \in \mathbb{Z}$, portanto r é par; contudo por hipótese r é ímpar e chegamos a uma contradição; assim $r = n^t$. ■

§ 4 A validade de (3.22) para $p \geqslant 3$

Nesse parágrafo introduziremos Somas de Jacobi quando p for um número primo ímpar. Congruências com Somas de Jacobi serão utilizadas aqui com o objetivo de reformular a condição (3.22); nela temos $T(X)^{(n-\sigma_n)\cdot\beta} \equiv \zeta \bmod N$ com N ideal de B e $B = \mathbb{Z}[\zeta_p k, \zeta_q]\left[\frac{1}{q}\right]$. Através dessas Somas passaremos a trabalhar com elementos de $\mathbb{Z}[\zeta_p k]$ que é um subanel de B.

Sejam como nos parágrafos anteriores p, q números primos; k, n números naturais; $p^k/(q-1)$; $X : F_q^* \longrightarrow \langle \zeta_p k \rangle$; $G = \{\sigma_x : 1 \leqslant x \leqslant p^k,\ x \not\equiv 0 \bmod p\}$ e $T(X) = \sum_{x=1}^{q-1} X(x).(\zeta_q)^x$. Lembremos que X pode ser extendida a Z fazendo-se para todo $z \in Z$ $X(z) = X(z \bmod q)$ e $X(0) = 0$.

Sejam a e b dois números inteiros. A Soma de Jacobi $j(X^a, X^b)$ associada aos caracteres X^a e X^b é um elemento de $\mathbb{Z}[\zeta_p k]$ definido por:

$$(4.1)\quad j(X^a, X^b) = \sum_{x=0}^{q-1} X^a(x).X^b(1-x)$$

Juntaremos agora algumas técnicas na seguinte proposição:

(4.2) PROPOSIÇÃO: Seja $X : F_q^* \longrightarrow U_p k$ função caracter de ordem p^k. Se r é um número inteiro tal que $r \not\equiv 0 \bmod p^k$ então $\sum_{x=1}^{q-1} X^r(x) = 0$.

PROVA: Lembremos que F_q^* é um grupo cíclico de ordem q-1 onde $q-1 = p^k.s$ com $s \in Z_+$. Seja y gerador de F_q^*, então $X(y) = \zeta_p k$, assim, dado $r \in Z$ com $r \not\equiv 0 \bmod p^k$ temos $X^r(y) = (\zeta_p k)^r \neq 1$. Se p^h

é a ordem de X^r temos $(X^r(y))^{p^h} = X^r(y^{p^h}) = 1$, logo $X^r(y)$ é uma raiz p^h-ésima primitiva da unidade. Sabemos no entanto que a soma de todas as raízes p^h-ésimas da unidade é igual a zero consequentemente $\sum_{i=1}^{p^h}(X^r(y))^i = 0$. Como $\sum_{x=1}^{q-1}X^r(x) = \sum_{t=1}^{q-1}X^r(y^t)$ e X é um homomorfismo encontramos $\sum_{t=1}^{q-1}X^r(y^t) = \sum_{t=1}^{p^k}(X^r(y))^t =$ $= \sum_{j=0}^{p^{k-h}(s-1)}((X^r(y))^j)^{p^h} \cdot \sum_{i=1}^{p^h}(X^r(y))^i = 0$, portanto $\sum_{x=1}^{q-1}X^r(x) = 0$. ∎

Consequentemente

(4.3) Se $a,b \in Z$ com $a + b \not\equiv 0 \bmod p^k$ temos $\sum_{x=1}^{q-1}X^a(x).X^b(-x) = X(-1).\sum_{x=1}^{q-1}X^{a+b}(x) = 0$ e

(4.4) Se $b \not\equiv 0 \bmod p^k$ então $\sum_{x=0}^{q-1}X^b(1-x) = 0$ pois existe uma bijeção entre x e 1-x de modo que se identificarmos 1-x com (1-x) mod q é fácil observar que quando x percorre F_q, 1-x também percorre F_q, assim $\sum_{x=0}^{q-1}X^b(1-x) = \sum_{x=0}^{q-1}X^b(x) = \sum_{x=1}^{q-1}X^b(x) = 0$. ∎

A seguir relacionaremos Somas de Jacobi com Somas de Gauss.

(4.5) LEMA: Sejam a,b números inteiros. Se $(a + b) \not\equiv 0 \bmod p^k$ então $j(X^a,X^b) = (T(X^a).T(X^b))/T(X^{a+b})$.

PROVA: Por hipótese $a + b \not\equiv 0 \bmod p^k$ de modo que ou ambos a e b não são côngruos a zero módulo p^k ou somente um deles é côngruo a zero módulo p^k. Suponhamos primeiramente que $a \equiv 0 \bmod p^k$, ou seja, a é múltiplo de p^k. Desde que X é um caracter de ordem p^k, teremos $X^a = 1$ o que implica em $T(X^a) = \sum_{x=1}^{q-1}(\zeta_q)^x$; no entanto a soma das raízes q-ésimas da unidade é igual a zero de modo que

(4.6) $T(X^a) = \sum_{x=0}^{q-1}(\zeta_q)^x - (\zeta_q)^0 = -1$

Por outro lado observemos que

(4.7) $T(X^{a+b}) = T(X^b.1) = T(X^b)$

Notemos agora que $j(X^a,X^b) = \sum_{x=0}^{q-1}X^a(x).X^b(1-x) =$ $= \sum_{x=1}^{q-1}X^b(1-x)$ pois $X^a(0) = 0$, mas constatamos por (4.4) que $\sum_{x=0}^{q-1}X^b(1-x) = 0$ logo

(4.8) $j(X^a,X^b) = \sum_{x=0}^{q-1}X^b(1-x) - X^b(1) = -1$

Utilizando as igualdades (4.6), (4.7) e (4.8) obteremos $(T(X^a).T(X^b))/T(X^{a+b}) = -T(X^b)/T(X^b) = -1 = j(X^a,X^b)$ e assim provamos o lema para $a \equiv 0 \bmod p^k$.

Suponhamos agora $a \not\equiv 0 \bmod p^k$ e $b \not\equiv 0 \bmod p^k$. Dado $c \in Z$, $T(X^c) = \sum_{x=1}^{q-1}X^c(x).(\zeta_q)^x = \sum_{x=0}^{q-1}X^c(x).(\zeta_q)^x$ visto que $X^c(0) = 0$; assim $T(X^a).T(X^b) = (\sum_{x=0}^{q-1}X^a(x).(\zeta_q)^x).(\sum_{y=0}^{q-1}X^b(y).(\zeta_q)^y) =$ $= \sum_{x=0}^{q-1}\sum_{y=0}^{q-1}X^a(x).X^b(y).(\zeta_q)^{x+y}$. Notemos que na somatória y percorre F_q, assim para cada x fixado podemos identificar y-x com (y-x) mod q de modo que y-x também percorre F_q, portanto podemos substituir na igualdade acima y por y-x obtendo

(4.9) $T(X^a).T(X^b) = \sum_{y=0}\sum_{x=0}X^a(x).X^b(y-x).(\zeta_q)^y =$ $\sum_{y=1}^{q-1}\sum_{x=0}^{q-1}X^a(x).X^b(y-x).(\zeta_q)^y + \sum_{x=0}^{q-1}X^a(x).X^b(-x)$ pois para $y = 0$, $X^b(y-x) = X^b(-x)$.

No entanto, por (4.3) $\sum_{x=0}^{q-1}X^a(x).X^b(-x) = 0$, logo

(4.10) $T(X^a).T(X^b) = \sum_{y=1}^{q-1}\sum_{x=0}^{q-1}X^a(x).X^b(y-x).(\zeta_q)^y$

Agora $1 \leqslant y \leqslant q-1$, isto é, $y \in F_q^*$ e existe y^{-1} em F_q^*. Seja $x.y^{-1} = z$, ou melhor, $x = y.z$. Claramente para cada y fixado, quando x percorre F_q z também percorre F_q. Identificando-se z com z mod q temos $z \in Z_+$ com $0 \leqslant z \leqslant q-1$; de modo análogo podemos iden-

tificar y.z com y.z mod q. Substituindo esse novo valor de x em (4.10) teremos $T(X^a).T(X^b) = \sum_{y=1}^{q-1}\sum_{z=0}^{q-1} X^a(y.z).X^b(y - y.z).(\zeta_q)^y$ e a somatória acima é equivalente a $\sum_{y=1}^{q-1}\sum_{z=0}^{q-1} X^{a+b}(y).(\zeta_q)^y.X^a(z).X^b(1-z) =$ $= (\sum_{y=1}^{q-1} X^{a+b}(y).(\zeta_q)^y).(\sum_{z=0}^{q-1} X^a(z).X^b(1-z)) = T(X^{a+b}).j(X^a,X^b)$, logo $T(X^a).T(X^b) = T(X^{a+b}).j(X^a,X^b)$. Já provamos anteriormente que $T(X)$ é inversível portanto

(4.11) $j(X^a,X^b) = (T(X^a).T(X^b))/T(X^{a+b})$ se $(a + b) \not\equiv 0 \bmod p^k$. ∎

(4.12) PROPOSIÇÃO: Se $a.b.(a + b) \not\equiv 0 \bmod p$ então a igualdade $j(X^a,X^b) = (T(X^a).T(X^b))/T(X^{a+b})$ pode ser escrita como $j(X^a,X^b) = T(X)^{\sigma_a+\sigma_b-\sigma_{a+b}}$.

PROVA: Primeiramente observemos que dado $r \in Z$, existem s,t com $s \in Z_+$, $1 \leqslant s < p^k$ e $t \in Z$ tais que $r = s + t.p^k$, assim se $r \not\equiv 0 \bmod p$ teremos $s \not\equiv 0 \bmod p$ e σ_s será um automorfismo de $Q(\zeta_{p^k},\zeta_q)$ pertencente ao grupo G descrito no parágrafo anterior. Notemos no entanto que $(\zeta_{p^k})^r = (\zeta_{p^k})^s$, logo se definirmos $\sigma_r(\zeta_{p^k}) = (\zeta_{p^k})^r$ e $\sigma_r(\zeta_q) = \zeta_q$, σ_r será um automorfismo equivalente a σ_s. A partir daí faz sentido $T(X)^{\sigma_r} = \sigma_r(T(X)) =$ $= \sigma_r(\sum_{x=1}^{q-1} X(x).(\zeta_q)^x)$. Como $X(x) \in U_{p^k}$ temos $\sigma_r(X(x)) = X(x)^r$, além disso $\sigma_r((\zeta_q)^x) = (\zeta_q)^x$, logo $\sigma_r(\sum_{x=1}^{q-1} X(x).(\zeta_q)^x) = \sum_{x=1}^{q-1} X^r(x).(\zeta_q)^x = T(X^r)$, portanto se $r \not\equiv 0 \bmod p$, $T(X^r) = T(X)^{\sigma_r}$. Na presente proposição temos por hipótese $a.b.(a + b) \not\equiv 0 \bmod p$, ou seja, $a \not\equiv 0 \bmod p$, $b \not\equiv 0 \bmod p$, $(a + b) \not\equiv 0 \bmod p$, então $j(X^a,X^b) = (T(X^a).T(X^b))/T(X^{a+b}) =$ $= (T(X)^{\sigma_a}.T(X)^{\sigma_b})/T(X)^{\sigma_{a+b}}$, mas já provamos que $T(X)^{-1} \in B$, logo

(4.13) $j(X^a,X^b) = T(X)^{\bar{\sigma}_a+\bar{\sigma}_b-\bar{\sigma}_{a+b}}$ se $a.b.(a+b) \not\equiv 0 \bmod p$. ∎

Observemos que $p = 2$ implica em $a.b.(a+b) \equiv 0 \bmod p$ para todo $a,b \in \mathbb{Z}$, portanto a hipótese da Proposição (4.12) exclui o primo $p = 2$.

Introduziremos aqui duas notações:

(4.14) Dado um número real y, $[y]$ irá denotar o maior número inteiro menor ou igual a y.

(4.15) Dado p número primo $p \geq 3$, $W = \{x \in \mathbb{Z} \;/\; 1 \leq x \leq p^k, x \not\equiv 0 \bmod p\}$.

(4.16) Utilizaremos a partir daqui um ideal M de $\mathbb{Z}[\zeta_{p^k}]$ satisfazendo as seguintes condições: $M \cap \mathbb{Z} = n\mathbb{Z}$ e $\bar{\sigma}_n[M] = M$. É fácil observar que o ideal $n\mathbb{Z}[\zeta_{p^k}]$ preenche as condições desejadas, logo tal M existe; contudo, por motivos ligados a computação, é conveniente encontrar o maior ideal possível. Existem alguns métodos para construir tal ideal, no entanto aqui iremos apenas assegurar a existência de tal ideal. Sabemos que $\mathbb{Z}[\zeta_{p^k}]$ é um anel Noetheriano, portanto toda família não vazia de ideais de $\mathbb{Z}[\zeta_{p^k}]$ possui um ideal maximal; assim sendo existe um ideal maximal M contendo $n\mathbb{Z}[\zeta_{p^k}]$ tal que $M \cap \mathbb{Z} = n\mathbb{Z}$ e $\bar{\sigma}_n[M] = M$.

A partir daqui faremos demonstrações utilizando um ideal M genérico que satisfaça as condições acima, entretanto ressaltamos que para a aplicação do algorítmo deve ser escolhido o ideal maximal.

(4.17) PROPOSIÇÃO: Seja M um ideal de $Z[\zeta_p k]$ que satisfaz as seguintes condições: $M \cap Z = nZ$ e $\sigma_n[M] = M$. Se $N = \{(\sum_{j=0}^{q-2} a_j.(\zeta_q)^j).q^d : a_j \in M , (0 \leqslant j \leqslant q-2) , d \in Z\}$ então N é um ideal de $B = Z[\zeta_p k, \zeta_q]\left[\frac{1}{q}\right]$ e se $(q,n) = 1$ então $N \cap Z = nZ$ e $\sigma_n[N] = N$.

PROVA: Claramente N é um ideal de B.

Para provar que $N \cap Z = nZ$ é suficiente demonstrar que $N \cap Z[\zeta_p k] = M$ pois $N \cap Z = N \cap (Z[\zeta_p k] \cap Z) = (N \cap Z[\zeta_p k]) \cap Z$; assim se $N \cap Z[\zeta_p k] = M$ teremos $(N \cap Z[\zeta_p k]) \cap Z = M \cap Z$, mas por hipótese $M \cap Z = nZ$ portanto $N \cap Z = nZ$.

Verificaremos então que $N \cap Z[\zeta_p k] = M$.

Como N é gerado por M e M é ideal de $Z[\zeta_p k]$ temos $M \subset N \cap Z[\zeta_p k]$; falta contudo provar que $N \cap Z[\zeta_p k] \subset M$ e é o que faremos agora.

N é ideal de B, logo N é um subconjunto de $Q(\zeta_p k, \zeta_q)$.

Dado $x \in N \cap Z[\zeta_p k]$, $x = (\sum_{j=0}^{q-2} a_j.(\zeta_q)^j).q^d =$ $= \sum_{j=0}^{q-2}(a_j.q^d).(\zeta_q)^j$ e isso implica em $(q^d.a_0 - x) + \sum_{j=1}^{q-2}(a_j.q^d).(\zeta_q)^j = 0$.

Recordemos que $Q(\zeta_p k, \zeta_q)$ pode ser visto como um espaço vetorial sobre $Q(\zeta_p k)$ com dimensão q-1 e com base $\{1 , \zeta_q , \ldots , (\zeta_q)^{q-2}\}$.

Notemos agora que todos os coeficientes de $(\zeta_q)^j$, $0 \leqslant j \leqslant p-2$, na última igualdade pertencem a $Q(\zeta_p k)$; como $1 , \zeta_q , \ldots , (\zeta_q)^{q-2}$ são linearmente independentes sobre $Q(\zeta_p k)$ temos $(q^d.a_0 - x) + \sum_{j=1}^{q-2}(q^d.a_j).(\zeta_q)^j = 0$ se e somente se $a_j = 0$ pa-

ra $1 \leqslant j \leqslant q-2$ e $q^d.a_0 = x$.

Se $d \geqslant 0$ teremos $q^d \in Z$ o que implica em $q^d.a_0 \in M$, portanto $x \in M$.

Se $d < 0$, seja $a_0 = \sum_{\substack{0\leqslant i\leqslant p^k \\ i\not\equiv 0 \bmod p}} y_i.(\zeta_p k)^i$ com $y_i \in Z$ e $y_i = q^{e_i}.y_i'$, $y_i' \in Z$, $(y_i', q) = 1$. Seja $c = \min(e_i) \geqslant 0$, então $a_0 = q^c.\sum_{\substack{0\leqslant i\leqslant p^k \\ i\not\equiv 0 \bmod p}} (q^{e_i-c}.y_i').(\zeta_p k)^i$, logo $a_0 = q^c.a'$ onde $a' = \sum_{\substack{0\leqslant i\leqslant p^k \\ i\not\equiv 0 \bmod p}} q^{e_i-c}.y_i'.(\zeta_p k)^i \in Z[\zeta_p k]$.

Desde que $(n,q) = 1$ existem $s,t \in Z$ tais que $q^c.s + n.t = 1$. Multiplicando os dois lados da igualdade por a' encontramos $a'.q^c.s + a'.n.t = a'$. Observemos que $a'.q^c = a_0 \in M$ logo $a'.q.s \in M$; também $n \in M$ de modo que $a'.n.t \in M$, portanto $a' \in M$.

$x = a_0.q^d = a'.q^{c+d}$.

Se $c + d \geqslant 0$ teremos $q^{c+d} \in Z$, logo $a'.q^{c+d} \in M$ e então $x \in M$.

Provaremos a seguir que o caso $c + d < 0$ não ocorre, pois se $c + d < 0$ então $x \notin Z[\zeta_p k]$.

$x = a_0.q^d = \sum_{\substack{0\leqslant i\leqslant p^k \\ i\not\equiv 0 \bmod p}} q^{e_i+d}.y_i'.(\zeta_p k)^i$.

Se $c + d < 0$ então para algum i, $e_i + d < 0$, mas $(y_i', q) = 1$ o que implica em $q^{e_i+d}.y_i' \notin Z$. No entanto $x \in Z[\zeta_p k]$ e $(\zeta_p k)^i$ são linearmente independentes sobre Z quando $0 < i \leqslant p^k$ e $i \not\equiv 0 \bmod p$ de modo que se um dos coeficientes não pertence a Z então $x \notin Z[\zeta_p k]$.

Para provar que $\sigma_n^-[N] = N$, seja $x = (\sum_{j=0}^{q-2} a_j.(\zeta_q)^j).q^d \in N$ assim $\sigma_n^-(x) = (\sum_{j=0}^{q-2} \sigma_n^-(a_j).(\zeta_q)^j).q^d$ visto que σ_n^- atua apenas nas raizes p^k-ésimas da unidade; mas, por hipótese, $\sigma_n^-[M] = M$ o que

implica em $\sigma_n^-(a_j) \in M$ qualquer que seja j, $0 \leqslant j \leqslant q-2$, portanto $\sigma_n^-(x) \in N$, isto é, $\sigma_n^-[N] \subset N$. Observemos no entanto que σ_n^- é um automorfismo de ordem finita, logo $N \subset \sigma_n^-[N]$ e então $\sigma_n^-[N] = N$. ∎

O último resultado necessário para a prova do Teorema (4.31) será o Lema (4.24); porém para que a demonstração desse Lema seja mais objetiva enunciaremos agora pequenas proposições que nos auxiliarão na prova da segunda afirmação do Lema em questão. São elas:

(4.18) PROPOSIÇÃO: Qualquer que seja $x \in W$ com $W = \{x \in Z : 1 \leqslant x \leqslant p^k , x \not\equiv 0 \bmod p\}$, $x^{-1} \in Z_p$.

PROVA: Desde que $W \subset Z$, W pode ser visto como um subconjunto de de Z_p. Lembremos no entanto que $a \in Z_p^*$ se e somente se $a \not\equiv 0 \bmod p$ de modo que $W \subset Z_p^*$ e então todo elemento de W possui inverso x^{-1} em Z_p. ∎

(4.19) PROPOSIÇÃO: Seja $a \in Z_p$ tal que $a \equiv p^{k-1} \bmod p^k$; então $v_p(a) = k - 1$.

PROVA: Se $a \equiv p^{k-1} \bmod p^k$ então $a = p^{k-1} + p^k.t =$ $= p^{k-1}.(1 + p.t)$. Como $1 + p.t \in 1 + pZ_p$, $v_p(1 + p.t) = 0$, logo $v_p(a) = v_p(p^{k-1}) + v_p(1 + p.t) = k - 1$. ∎

(4.20) PROPOSIÇÃO: Se $H = \{y \in Z \ / \ 0 \leqslant y \leqslant p^k$ e $y \equiv 1 \bmod p\}$ então $\sum_{y \in H} y = p^{k-1} + \frac{1}{2}.p^k.(p^{k-1} - 1)$.

PROVA: $H = \{1 + p.j \;/\; 0 \leqslant j \leqslant p^{k-1} - 1\}$ de modo que $\sum_{y\in H} y = \sum_{j=0}^{p^{k-1}-1}(1 + j.p) = \sum_{j=0}^{p^{k-1}-1} 1 + p.\sum_{j=0}^{p^{k-1}-1} j$. Observemos no entanto que $\sum_{j=0}^{p^{k-1}-1} 1 = p^{k-1}$ e que $\sum_{j=0}^{p^{k-1}-1} j$ corresponde à soma dos primeiros p^{k-1} termos de uma Progressão Aritmética de razão 1, portanto $\sum_{j=0}^{p^{k-1}-1} j = (p^{k-1} - 1).p^{k-1}/2$ e $p.\sum_{j=0}^{p^{k-1}-1} j = p^k.(p^{k-1} - 1)/2$. Temos então $\sum_{y\in H} j = p^{k-1} + p^k.(p^{k-1} - 1)/2$. Adicionalmente, notemos que $p^{k-1} - 1$ é um número par, consequentemente $(p^{k-1} - 1)/2 = w \in N$ e $\sum_{y\in H} y = p^{k-1} + p^k.w$. ■

(4.21) PROPOSIÇÃO: Seja $W = \{x \in Z : 1 \leqslant x \leqslant p^k \;,\; x \not\equiv 0 \bmod p\}$ então $v_p(\sum_{x\in W} x^{1-p}) = k - 1$.

PROVA: Já provamos na Proposição (4.18) que $x^{-1} \in Z_p^*$ logo x^{-p} também pertence a Z_p^* e $x^{1-p} = (a_i \bmod p^i)_{i=1}^{\infty} \in Z_p^*$. Seja $y_i \in Z$, $0 \leqslant y_i < p^i$ onde $\bar{y}_i = a_i \bmod p^i \in Z/p^iZ$; temos assim $x^{1-p} = (\bar{y}_i)_{i=1}^{\infty}$ e $x^{1-p} \bmod p^k = \bar{y}_k$. Notemos agora que $x^{1-p}.x^{p-1} = 1$ em Z_p e pelo Teorema de Fermat $x^{p-1} \equiv 1 \bmod p$ o que implica em $x^{1-p} \equiv 1 \bmod p$, então $y_j \equiv 1 \bmod p$ para todo $j \in Z_+^*$. Seja $\bar{H} = \{\bar{y} \in (Z/p^kZ)^* \;:\; y \equiv 1 \bmod p\}$. Claramente $\bar{H}$ tem ordem p^{k-1}. Notemos contudo que $y_k \equiv 1 \bmod p$, assim $\bar{y}_k \in \bar{H}$ e os valores assumidos por $x^{1-p} \bmod p^k$ são precisamente os elementos de $\bar{H}$. Desde que $\bar{H}$ é um subgrupo de índice p-1 do grupo cíclico $(Z/p^kZ)^*$, a cada $\bar{y} \in \bar{H}$ correspondem p-1 elementos $x^{1-p} \bmod p^k$ com $x \in W$. Assim $\sum_{x\in W} x^{1-p} \equiv (p - 1).\sum_{y\in H} y \bmod p^k$. Pela Proposição (4.20) $\sum_{y\in H} y = p^{k-1} + p^k.(p^{k-1} - 1)/2$ o que implica em $\sum_{x\in W} x^{1-p} = (p - 1).(p^{k-1} + p^k.(p^{k-1} - 1)/2) \bmod p^k$ portanto

$\sum_{x \in W} x^{1-p} \equiv -p^{k-1} \bmod p^k$ e pela Proposição (4.19) obtemos $v_p(\sum_{x \in W} x^{1-p}) = k - 1$. ■

(4.22) PROPOSIÇÃO: Dados $x,y \in \mathbb{Z}$, se $x \equiv y \bmod p^k$ então $x^p \equiv y^p \bmod p^{k+1}$.

PROVA: Seja $x = a + r.p^k$ e $y = a + s.p^k$ com $a,r,s \in \mathbb{Z}$ e $0 \leqslant a < p^k$. $x^p = (a + r.p^k)^p = a^p + \sum_{i=1}^{p} \binom{p}{i} . a^{p-i} . (r.p^k)^i$, mas para $1 \leqslant i < p$ $p/\binom{p}{i}$ e $p^k/(p^k)^i$ e para $i = p$, $p^{k+1}/(p^k)^i$, portanto para $i \geqslant 1$ $p^{k+1}/\sum_{i=1}^{p} \binom{p}{i} . a^{p-i} . (r.p^k)^i$, logo $\sum_{i=1}^{p} \binom{p}{i} . a^{p-i} . (r.p^k)^i = t.p^{k+1}$, $t \in \mathbb{Z}$ e então $x^p = a^p + t.p^{k+1}$. De modo análogo $y^p = a^p + u.p^{k+1}$. Assim $x^p - y^p = p^{k+1}.(t - u)$ o que implica em $x^p \equiv y^p \bmod p^{k+1}$. ■

(4.23) PROPOSIÇÃO: Seja $G = \{\sigma_x : 1 \leqslant x \leqslant p^k , x \not\equiv 0 \bmod p\}$. Existe um homomorfismo de anéis $\varphi : \mathbb{Z}[G] \longrightarrow \mathbb{Z}/p^{k+1}\mathbb{Z}$ tal que para todo $\sigma_x, \sigma_y \in G$, $n_x, n_y \in \mathbb{Z}$, $\varphi(n_x.\sigma_x + n_y.\sigma_y) = (n_x.x^p + n_y.y^p) \bmod p^{k+1}$.

PROVA: Inicialmente lembremos que a operação definida em G é a composição, assim dados $\sigma_x, \sigma_y \in G$, $\sigma_x o \sigma_y(\zeta_p k) = \sigma_x((\zeta_p k)^y) = (\zeta_p k)^{x.y}$, logo se $z \in \mathbb{Z}_+$, $1 \leqslant z \leqslant p^k$ e $z \equiv x.y \bmod p^k$ teremos $\sigma_x o \sigma_y(\zeta_p k) = (\zeta_p k)^z = \sigma_z(\zeta_p k)$ com $\sigma_z \in G$. A partir daí $\varphi(\sigma_x o \sigma_y) = \varphi(\sigma_z) = z^p \bmod p^{k+1}$, mas pela Proposição (4.22) $z^p \equiv (y.x)^p \bmod p^{k+1}$ de modo que $\varphi(\sigma_x o \sigma_y) = (x.y)^p \bmod p^{k+1} = x^p \bmod p^{k+1}.y^p \bmod p^{k+1}$, isto é, $\varphi(\sigma_x o \sigma_y) = \varphi(\sigma_x).\varphi(\sigma_y)$. Sejam $a = \sum_{x \in W} n_x.\sigma_x$, $b = \sum_{x \in W} m_x.\sigma_x$, $c = \sum_{x \in W} n_y.\sigma_y$, $a,b,c \in \mathbb{Z}[G]$. $\varphi(a + b) = \varphi(\sum_{x \in W} (n_x + m_x).\sigma_x) =$

$= (\sum_{x\in W}(n_x + m_x).x^p) \bmod p^{k+1} = \sum_{x\in W} n_x.x^p \bmod p^{k+1} +$

$+ \sum_{x\in W} m_x.x^p \bmod p^{k+1} = \Psi(a) + \Psi(b)$. $\Psi(a.c) = \Psi(\sum_{x\in W} n_x.\sigma_x.\sum_{y\in W} n_y.\sigma_y) =$

$= \Psi(\sum_{z\in W} n_z.\sigma_z)$ onde $n_{z_{x.y \bmod p^k}} = \sum n_x.n_y$, logo $\Psi(\sum_{z\in W} n_z.\sigma_z) =$

$= (\sum_{z\in W} n_z.z^p) \bmod p^{k+1} = (\sum_{x,y\in W} n_x.n_y.(x.y)^p) \bmod p^{k+1} =$

$= (\sum_{x\in W} n_x.x^p.\sum_{y\in W} n_y.y^p) \bmod p^{k+1}$, portanto $\Psi(a.c) = \Psi(a).\Psi(c)$ e constatamos que Ψ é homomorfismo. ∎

(4.24) LEMA: Sejam $a,b \in Z$ com $(a + b)^p \not\equiv (a^p + b^p) \bmod p^2$ e $a.b.(a + b) \not\equiv 0 \bmod p$. Para n número natural tal que $(n,p.q) = 1$ seja $\alpha = \sum_{x\in W}[n.x/p^k].(\sigma_x)^{-1}$ e $\beta = \sum_{x\in W}([(a+b).x/p^k] - [a.x/p^k] - [b.x/p^k]).(\sigma_x)^{-1}$. Então $(n - \sigma_n).\beta = (\sigma_a + \sigma_b - \sigma_{a+b}).\alpha$ em $Z[G]$ e β satisfaz (3.15): $(\zeta_p)^\beta \neq 1$.

PROVA: Antes de dar início à demonstração do Lema, provaremos que $(\sigma_x)^{-1} = \sigma_{x^{-1}} \bmod p^k$ (onde $x^{-1} \bmod p^k = (x \bmod p^k)^{-1}$) pois esse resultado nos dará maior liberdade para trabalhar com $(\sigma_x)^{-1}$. Sabemos que se $x \in W$ ($W = \{x \in Z : 1 \leqslant x \leqslant p^k, x \not\equiv 0 \bmod p\}$) então $\sigma_x \in G$ e $\sigma_x(\zeta_p k) = (\zeta_p k)^x$ e $\sigma_x(\zeta_q) = \zeta_q$; seja $\sigma_s = (\sigma_x)^{-1}$, logo $\sigma_s o \sigma_x(\zeta_p k) = \zeta_p k$; assim $\sigma_s o \sigma_x(\zeta_p k) = (\zeta_p k)^{x.s} = \zeta_p k$, isto é, $x.s \equiv 1 \bmod p^k$ e encontramos $s \equiv x^{-1} \bmod p^k$ com $s \in W$ ($s \bmod p^k = (x \bmod p^k)^{-1}$; chamaremos a esse $s \in W$ de x^{-1}); portanto $(\sigma_x)^{-1} = \sigma_s = \sigma_{x^{-1}} \bmod p^k$.

Para provar a primeira asserção do Lema vamos definir $\theta = \sum_{x\in W} x.(\sigma_x)^{-1} \in Z[G]$.

Seja $m \in Z$, $m \not\equiv 0 \bmod p$ fixado; seja $x \equiv m.y \bmod p^k$; como $x^{-1} \bmod p^k$ e $y^{-1} \bmod p^k$ pertencem a $(Z/p^k)^* \simeq W$, temos

$y^{-1} \equiv m.x^{-1} \bmod p^k$.

Seja $r(m.y)$ o resto da divisão de $m.y$ por p^k, de modo que $m.y = [m.y/p^k].p^k + r(m.y)$, com $r(m.y) < p^k$, logo de $x \equiv m.y \bmod p^k$ obtemos $x \equiv r(m.y) \bmod p^k$, ou seja p^k divide $(x - r(m.y))$; no entanto $x \leqslant p^k$ e $r(m.y) < p^k$, então $x - r(m.y) < p^k$ o que implica em $x = r(m.y)$. Assim $\sigma_m.\theta = \sum_{x\in W} x.\sigma_m o(\sigma_x)^{-1} = \sum_{y\in W} r(m.y).(\sigma_y)^{-1}$. Notemos que quando x percorre W, y também percorre W de modo que $\sum_{x\in W} x.(\sigma_x)^{-1} = \sum_{y\in W} y.(\sigma_y)^{-1}$, logo $(m - \sigma_m).\theta = \sum_{y\in W} m.y.(\sigma_y)^{-1} - \sum_{y\in W} r(m.y).(\sigma_y)^{-1} =$

$= \sum_{y\in W} (m.y - r(m.y)).(\sigma_y)^{-1}$, mas $m.y - r(m.y) = [m.y/p^k].p^k$, portanto

$$(4.25) \quad (m-\sigma_m).\theta = p^k.\sum_{y\in W}[m.y/p^k].(\sigma_y)^{-1}$$

Como $n \not\equiv 0 \bmod p$, n também satisfaz a igualdade acima e substituindo-se m por n encontramos

$$(4.26) \quad (n - \sigma_n).\theta = p^k.\sum_{y\in W}[n.y/p^k].(\sigma_y)^{-1} = p^k.\alpha$$

visto que $\alpha = \sum_{x\in W}[n.x/p^k].(\sigma_x)^{-1} = \sum_{y\in W}[n.y/p^k].(\sigma_y)^{-1}$.

Notemos agora que se substituírmos sucessivamente m em (4.25) por a+b , a , b encontraremos:

$(\sigma_a + \sigma_b - \sigma_{a+b}).\theta = ((a + b - \sigma_{a+b}) - (a - \sigma_a) - (b - \sigma_b)).\theta =$

$= p^k.\sum_{y\in W}[(a + b).y/p^k].(\sigma_y)^{-1} - p^k.\sum_{y\in W}[a.y/p^k].(\sigma_y)^{-1} -$

$- p^k.\sum_{y\in W}[b.y/p^k].(\sigma_y)^{-1}$ e pela definição de β:

$$(4.27) \quad (\sigma_a + \sigma_b - \sigma_{a+b}).\theta = p^k.\beta$$

Se combinarmos essa última igualdade com (4.26) teremos

$p^k.(n - \sigma_n).\beta = (n - \sigma_n).(p^k.\beta) = (n - \sigma_n).(\sigma_a + \sigma_b - \sigma_{a+b}).\theta =$

$= (\sigma_a + \sigma_b - \sigma_{a+b}).(n - \sigma_n).\theta = (\sigma_a + \sigma_b - \sigma_{a+b}).p^k.\alpha =$

$= p^k.(\bar{\sigma}_a + \bar{\sigma}_b - \bar{\sigma}_{a+b}).\alpha$, isto é,

(4.28) $p^k.(n - \bar{\sigma}_n).\beta = p^k.(\bar{\sigma}_a + \bar{\sigma}_b - \bar{\sigma}_{a+b}).\alpha$

Notemos entretanto que $Z[G]$ é livre de torção de modo que para todo $x \in Z[G]$ e $y \in Z$, $y.x = 0$ implica em $y = 0$ ou $x = 0$; concluímos daí que a igualdade (4.28) é equivalente a $(n - \bar{\sigma}_n).\beta = (\bar{\sigma}_a + \bar{\sigma}_b - \bar{\sigma}_{a+b}).\alpha$ e provamos assim a primeira afirmação do Lema.

Já vimos em (3.17) que a condição (3.15): $(\zeta_p)^\beta \neq 1$ é equivalente a $\sum_{x\in I} n_x.x \not\equiv 0 \bmod p^k$ para $\beta = \sum_x n_x.\bar{\sigma}_x \in Z[G]$; logo provar que $\beta = \sum_{x\in W}([(a + b).x/p^k] - [a.x/p^k] - [b.x/p^k]).(\bar{\sigma}_x)^{-1}$ pertence a $Z[G]$ satisfaz $(\zeta_p)^\beta \neq 1$ é equivalente a provar que $\sum_{x\in W}([(a + b).x/p^k] - [a.x/p^k] - [b.x/p^k]).x^{-1} \not\equiv 0 \bmod p$, considerando o lado esquerdo da congruência como um elemento de Z_p.

Provamos em (4.23) que existe um homomorfismo de anéis $\varphi : Z[G] \longrightarrow Z/p^{k+1}Z$ tal que para todo $\bar{\sigma}_x, \bar{\sigma}_y \in G$, $n_x, n_y \in Z$ temos $\varphi(n_x.\bar{\sigma}_x + n_y.\bar{\sigma}_y) = (n_x.x^p + n_y.y^p) \bmod p^{k+1}$. Aplicando esse homomorfismo a (4.27) : $(\bar{\sigma}_a + \bar{\sigma}_b - \bar{\sigma}_{a+b}).\theta = p^k.\beta$ obtemos

(4.29) $(a^p + b^p - (a + b)^p).\sum_{x\in W} x^{1-p} \equiv$

$= p^k.\sum_{x\in W}([(a + b).x/p^k] - [a.x/p^k] - [b.x/p^k]).x^{-p} \bmod p^{k+1}$

A partir da hipótese $(a + b)^p \not\equiv (a^p + b^p) \bmod p^2$, encontramos $v_p(a^p + b^p - (a + b)^p) = 1$; de acordo com (4.21) $v_p(\sum_{x\in W} x^{1-p}) = k - 1$, portanto $v_p((a^p + b^p - (a + b)^p).\sum_{x\in W} x^{1-p}) = k$.

Notemos agora que se utilizarmos a argumentação análoga à Proposição (4.19) ($a \equiv p^{k-1} \bmod p^k$ então $v_p(a) = k - 1$) em (4.29) encontramos

$v_p(p^k) + v_p(\sum_{x\in W}([(a + b).x/p^k] - [a.x/p^k] - [b.x/p^k]).x^{-p}) = k$, lo

go $v_p(\sum_{x\in W}([(a+b).x/p^k] - [a.x/p^k] - [b.x/p^k]).x^{-p}) = 0$ e isso implica em

(4.30) $\sum_{x\in W}([(a+b).x/p^k] - [a.x/p^k] - [b.x/p^k]).x^{-p} \not\equiv 0 \bmod p$

Visto que todo $x \in W$ satisfaz o Teorema de Fermat $x^{p-1} \equiv 1 \bmod p$, claramente $x^{-p} \equiv x^{-1} \bmod p$ e substituindo esse valor em (4.30) obtemos $\sum_{x\in W}([(a+b).x/p^k] - [a.x/p^k] - [b.x/p^k]).x^{-1} \not\equiv 0 \bmod p$ provando com isso o Lema. ∎

O Teorema que provaremos a seguir fornece, a partir de uma congruência com Soma de Jacobi, um critério para que a condição (3.22) seja satisfeita dado p primo maior que 2.

(4.31) TEOREMA: Supondo p número primo, $p \geqslant 3$, sejam a,b números inteiros satisfazendo

(4.32) $(a+b)^p \not\equiv (a^p + b^p) \bmod p^2$, $a.b.(a+b) \not\equiv 0 \bmod p$

e seja M o ideal de $Z[\zeta_p k]$ satisfazendo

(4.33) $M \cap Z = nZ$ e $\sigma_n[M] = M$

Seja $\alpha = \sum_{x\in W}[n.x.p^k].(\sigma_x)^{-1} \in Z[G]$. Se

(4.34) $j(X^a,X^b)^\alpha \equiv \zeta \bmod M$ para algum $\zeta \in U_p k$, então a condição (3.22) é satisfeita. Se (4.34) não ocorre então n é composto.

PROVA: Seja $N = \{(\sum_{j=0}^{q-2} a_j.(\zeta_q)^j).q^d : a_j \in M \ (0 \leqslant j \leqslant q-2) \ , \ d \in Z\}$ o ideal gerado por M e seja $\beta = \sum_{x\in W}([(a+b).x/p^k] - [a.x/p^k] - [b.x/p^k]).(\sigma_x)^{-1}$. De (4.13) temos $j(X^a,X^b) = T(X)^{\sigma_a+\sigma_b-\sigma_{a+b}}$, assim $j(X^a,X^b)^\alpha = T(X)^{(\sigma_a+\sigma_b-\sigma_{a+b}).\alpha}$; no Lema (4.24) provamos que

$(\sigma_a + \sigma_b - \sigma_{a+b}).\alpha = (n - \sigma_n).\beta$, logo $j(X^a,X^b)^{\alpha} = T(X)^{(n-\sigma_n).\beta}$.

Observemos agora que $M \subset N$ de modo que a congruência (4.34) também é válida módulo N, isto é, $j(X^a,X^b)^{\alpha} \equiv \zeta \bmod N$ para algum $\zeta \in U_p k$, ou equivalentemente $T(X)^{(n-\sigma_n).\beta} \equiv \zeta \bmod N$. Através da Proposição (4.17) constatamos que N satisfaz a condição (3.16) e a partir do Lema (4.24) temos β satisfazendo a condição (3.15).

Notemos então que estamos com todas as hipóteses da condição (3.22), ou seja, (3.22) é satisfeita e o teorema está provado.

Para provar que se (4.34) não ocorre então n é composto, observemos que se (4.34) não ocorre qualquer que seja $\zeta \in U_p k$ então $T(X)^{(n-\sigma_n).\beta} \not\equiv \zeta \bmod N$, qualquer que seja $\zeta \in U_p k$; em particular $T(X)^{(n-\sigma_n).\beta} \not\equiv X(n)^{-n.\beta} \bmod N$ pois $X(n)^{-n.\beta} \in U_p k$, mas pelo Corolário (3.14) essa última congruência só não ocorre para n composto.

§ 5 O caso p = 2

Nesse parágrafo como no parágrafo anterior nos propomos a reformular a condição (3.22). Serão estabelecidas relações entre Somas de Gauss e Somas de Jacobi. As congruências aqui exibidas serão congruências módulo M, com M ideal de $Z[\zeta_2 k]$ satisfazendo $M \cap Z = nZ$ e $\sigma_n[M] = M$ em vez de congruências módulo N com N ideal de $Z[\zeta_p k, \zeta_q]\left[\frac{1}{q}\right]$.

Cada um dos cinco teoremas que exporemos aqui apresenta uma congruência que se for satisfeita implica na validade da condição (3.22); se a mencionada congruência não ocorrer n será um número composto.

Recordemos que desde o início do texto estamos supondo $(n , p.q) = 1$, assim, para p = 2 n é necessariamente um número ímpar.

Antes de provarmos o primeiro teorema desse parágrafo daremos duas proposições cujos resultados serão utilizados nas provas dos teoremas.

(5.1) PROPOSIÇÃO: Dado $B = Z[\zeta_q]\left[\frac{1}{q}\right]$ serão válidas as seguintes igualdades:

i) $nB \cap Z = nZ$

ii) $\sigma_n[nB] = nB$

PROVA: Claramente $nZ \subset nB \cap Z$ pois $nZ \subset nB$ e $nZ \subset Z$. Para provar a outra inclusão observemos primeiramente que $\zeta_2 = -1$ de modo que para p = 2 e k = 1 temos $B = Z[\zeta_2 k, \zeta_q]\left[\frac{1}{q}\right] = Z[\zeta_q]\left[\frac{1}{q}\right]$ logo $B \subset Q(\zeta_q)$.

Seja $x \in nB \cap Z$; $x = n.\sum_{ij} a_{ij}.(\zeta_q)^j.q^i$ com i, j, $a_{ij} \in Z$ e $0 \leqslant j \leqslant q-2$. A igualdade acima é equivalente a $0 = n.\sum_i a_{i0}.q^i - x + \sum_{ij} n.a_{ij}.q^i.(\zeta_q)^j$. Desde que $Q(\zeta_q)$ pode ser visto como espaço vetorial de dimensão q-1 sobre Q e $\{1, \zeta_q, \ldots\ldots, (\zeta_q)^{q-2}\}$ é uma base desse espaço, temos $1, \zeta_q, \ldots\ldots, (\zeta_q)^{q-2}$ linearmente independentes sobre Q. Na última igualdade todos os coeficientes dos elementos $(\zeta_q)^j$ pertencem a Q, logo $n.a_{ij}.q^i = 0$ para todo $j \geqslant 1$ e isso implica em $a_{ij} = 0$ para todo $j \neq 0$. Então $n.\sum_i a_{i0}.q^i = x$ com $x \in Z$. É fácil observar que $\sum_i a_{i0}.q^i \in Z$, pois caso contrário $\sum_i a_{i0}.q^i = s/q^r$ com $-r = \min\{i\} < 0$ e $(s,q) = 1$; no entanto $(n,q) = 1$ o que implica em $n.s/q^r$ não pertencer a Z; assim $\sum_i a_{i0}.q^i \in Z$, logo $n.\sum_i a_{i0}.q^i = x$ com $x \in nZ$, portanto $nB \cap Z \subset nZ$. Para verificar que $\sigma_n[nB] = nB$ basta observar que σ_n nesse caso é a função identidade visto que $\sigma_n(\zeta_2) = \sigma_n(-1) = (-1)^n = -1$ pois n é ímpar. ∎

(5.2) PROPOSIÇÃO: Dado $B = Z[\zeta_4, \zeta_q]\left[\frac{1}{q}\right]$ são válidas as seguintes igualdades:

i) $nB \cap Z[\zeta_4] = nZ[\zeta_4]$

ii) $nB \cap Z = nZ$

iii) $\sigma_n[nB] = nB$

PROVA: Para verificar a primeira igualdade necessitamos apenas provar que $nB \cap Z[\zeta_4] \subset nZ[\zeta_4]$ pois a outra inclusão é óbvia. Observemos que $nB \subset Q(\zeta_4, \zeta_q)$ e $Q(\zeta_4, \zeta_q)$ pode ser visto como um espaço vetorial de dimensão q-1 sobre $Q(\zeta_4)$, tendo como base

$\{1, \zeta_q, \ldots, (\zeta_q)^{q-2}\}$. Seja x um elemento de $nB \cap Z[\zeta_4]$, $x = \sum_{i,j,t} n.a_{ijt}.(\zeta_4)^i.(\zeta_q)^j.q^t$; a_{ijt}, i, j, t $\in Z$; $i = 0, 1$; $0 \leqslant j \leqslant q-2$; então $0 = \sum_{i,t} n.a_{i0t}.(\zeta_4)^i.q^t - x + \sum_{\substack{i,t \\ x \neq j \neq q-2}} n.a_{ijt}.(\zeta_4)^i.(\zeta_q)^j.q^t$. Pelo fato de $1, \zeta_q, \ldots, (\zeta_q)^{q-2}$ serem linearmente independentes sobre $Q(\zeta_4)$ e $n.a_{ijt}.(\zeta_4)^i.q^t \in Q(\zeta_4)$, a igualdade acima acontece se e somente se $a_{ijt} = 0$ para todo i, j, t com $j \neq 0$ e $n.\sum_{i,t} a_{i0t}.q^t.(\zeta_4)^i - x = 0$ o que implica em $n.\sum_{i,t} a_{i0t}.q^t.(\zeta_4)^i = x$. De $x \in Z[\zeta_4]$ temos $x = a + b.\zeta_4$ com a, b $\in Z$ pois $\{1, \zeta_4\}$ é base de $Q(\zeta_4)$ sobre Q, portanto $n.\sum_t a_{00t}.q^t - a + (n.\sum_t a_{10t}.q^t - b).\zeta_4 = 0$; como $1, \zeta_4$ são linearmente independentes sobre Q e na igualdade acima seus coeficientes pertencem a Q encontramos $a = n.\sum_t a_{00t}.q^t \in Z$ e $b = n.\sum_t a_{10t}.q^t \in Z$ e com o procedimento idêntico ao utilizado na Proposição (5.1) obtemos $w = \sum_t a_{00t}.q^t \in Z$ e $u = \sum_t a_{10t}.q^t \in Z$; assim $x = n.w + n.u.\zeta_4 = n.(w + u.\zeta_4)$ onde $w + u.\zeta_4 \in Z[\zeta_4]$, então $x \in nZ[\zeta_4]$ portanto $nB \cap Z[\zeta_4] \subset nZ[\zeta_4]$.

Vamos agora verificar que $nB \cap Z = nZ$. Acabamos de provar que $nB \cap Z[\zeta_4] = nZ[\zeta_4]$ de modo que $nB \cap Z = nB \cap (Z[\zeta_4] \cap Z) = nZ[\zeta_4] \cap Z$ portanto provar que $nB \cap Z = nZ$ é equivalente a demonstrar que $nZ[\zeta_4] \cap Z = nZ$. Claramente $nZ \subset nZ[\zeta_4] \cap Z$; resta-nos então verificar a outra inclusão. Seja $y \in nZ[\zeta_4] \cap Z$, $y = n.(a + b.\zeta_4) \in Z$; a,b $\in Z$ logo $n.a - y + n.b.\zeta_4 = 0$, contudo sabemos que $1, \zeta_4$ são linearmente independentes sobre Q, consequentemente $n.a = y$ e $b = 0$, então $y = n.a \in nZ$, portanto $nZ[\zeta_4] \cap Z \subset nZ$.

A terceira igualdade $\sigma_n[nB] = nB$ é evidente pois $\sigma_n[nB] \subset nB$ e σ_n tem ordem finita o que implica em $nB \subset \sigma_n[nB]$, portanto temos a relação desejada. ∎

(5.3) TEOREMA: Seja $p = 2$ e $k = 1$. Se

(5.4) $q^{(n-1)/2} \equiv \zeta \bmod n$ para algum $\zeta \in \{1, -1\}$

então a condição (3.22) é satisfeita. Se (5.4) não ocorre então n é composto.

PROVA: Nesse caso temos $X : F_q^* \longrightarrow U_2$ com $U_2 = \{1, -1\}$, consequentemente X tem ordem 2, ou seja, $X = X^{-1}$. Em (3.9) provamos que $T(X).T(X^{-1}) = X(-1).q$, portanto aqui $T(X)^2 = X(-1).q$; assim $T(X)^{2.(n-1)} = (X(-1))^{n-1}.q^{n-1}$, mas $n-1$ é par de modo que $X(-1)^{n-1} = 1$ e $(n-1)/2 \in \mathbb{Z}_+$ o que implica em $q^{(n-1)/2} \in \mathbb{Z}_+$. Com isso $T(X)^{n-1} = \pm q^{(n-1)/2} \in \mathbb{Z}_+$. Observemos que $(\zeta_2)^n = \zeta_2$ (pois n é ímpar), assim $\sigma_n(\zeta_2) = \zeta_2$, portanto σ_n é a função identidade. Se tomarmos $\beta = 1 \in \mathbb{Z}[G]$ obteremos $T(X)^{(n-\sigma_n).\beta} = T(X)^{n-1} = \pm q^{(n-1)/2}$; usando (5.4) $(q^{(n-1)/2} = \zeta \bmod n)$ para $\zeta = 1$ ou $\zeta = -1$ temos $T(X)^{(n-\sigma_n).\beta} \equiv \zeta \bmod n$. Como $n \in nB$, se fizermos $N = nB$ encontraremos $T(X)^{(n-\sigma_n).\beta} \equiv \zeta \bmod N$ para algum $\zeta \in U_2$. Já provamos na Proposição (5.1) que $nB \cap \mathbb{Z} = n\mathbb{Z}$ e $\sigma_n[nB] = nB$ de modo que $N = nB$ satisfaz a condição (3.16); claramente $\beta = 1$ satisfaz (3.15): $(\zeta_2)^\beta = 1$ portanto a condição (3.22) é satisfeita.

Suponhamos agora que (5.4) não ocorre, isto é, $q^{(n-1)/2} \not\equiv \zeta \bmod n$ qualquer que seja $\zeta \in U_2$, mas $T(X)^{n-1} = \pm q^{(n-1)/2}$ de modo que $T(X)^{n-1} \not\equiv \zeta \bmod n$ para

$\zeta \in \{1, -1\}$, consequentemente $T(X)^{n-1} - \zeta \notin nZ$; entretanto $T(X)^{n-1} - \zeta \in Z$, logo $T(X)^{n-1} - \zeta \notin nB$ pois $Z \cap nB = nZ$; assim $T(X)^{n-1} \not\equiv \zeta \bmod nB$ qualquer $\zeta \in U_2$; em particular a relação acima é válida para $X(n)^{-n}$ que é uma raiz 2-ésima da unidade, isto é, $T(X)^{n-1} \not\equiv X(n)^{-n} \bmod nB$; tomando $\beta = 1$ encontraremos $T(X)^{(n-1).\beta} \not\equiv X(n)^{-n.\beta} \bmod nB$. Se n fosse primo, pelo Corolário (3.14) teríamos $T(X)^{(n-\sigma_n).\beta} \equiv X(n)^{-n.\beta} \bmod N$ para todo $\beta \in Z[G]$ e todo ideal N de B com $n \in N$, portanto n é composto. ∎

(5.5) TEOREMA: Seja $p = 2$, $k = 2$, $n \equiv 1 \bmod 4$ e M um ideal de $Z[\zeta_4]$ com $M \cap Z = nZ$. Se

(5.6) $j(X,X)^{(n-1)/2}.q^{(n-1)/4} \equiv \zeta \bmod M$ para algum $\zeta \in U_4$

então a condição (3.22) é satisfeita. Se (5.6) não ocorre então n é composto.

PROVA: Seja $N = \{(\sum_{j=0}^{q-2} a_j.(\zeta_q)^j).q^d : a_j \in M \ (0 \leqslant j \leqslant q-2),\ d \in Z\}$ o ideal de B gerado por M. Com procedimento idêntico ao utilizado na prova do Teorema (4.31) temos $N \cap Z[\zeta_4] = M$ e então $N \cap Z = N \cap Z[\zeta_4] \cap Z = M \cap Z = nZ$. De $n \equiv 1 \bmod 4$ temos $n = 1 + 4.x$ com $x \in Z$ de modo que $\sigma_n(\zeta_4) = (\zeta_4)^n = \zeta_4.((\zeta_4)^4)^x = \zeta_4$, assim σ_n é igual a identidade no gerador do grupo U_4, logo σ_n é o automorfismo identidade e portanto $\sigma_n[N] = N$.

Vimos em (3.9) que $T(X).T(X^{-1}) = X(-1).q$, logo $T(X^2).T(X^{-2}) = X^2(-1).q = q$ e nesse caso $X^2 = X^{-2}$ o que implica em $T(X^2)^2 = X^2(-1).q = q$ pois $X^2(-1) = 1$. Utilizando (4.11) temos $j(X,X) = (T(X).T(X))/T(X^2)$ visto que $(1 + 1) \not\equiv 0 \bmod 4$, então $T(X)^2 = j(X,X).T(X^2)$ e daí $T(X)^{n-\sigma_n} = T(X)^{n-1} = (T(X)^2)^{(n-1)/2} =$

$= (j(X,X).T(X^2))^{(n-1)/2} = j(X,X)^{(n-1)/2}.q^{(n-1)/4}$. Por (5.6) temos $j(X,X)^{(n-1)/2}.q^{(n-1)/4} \equiv \zeta \bmod M$ e essa congruência é equivalente a $T(X)^{n-\sigma_n} \equiv \zeta \bmod M$; como $M \subset N$ encontramos $T(X)^{n-\sigma_n} \equiv \zeta \bmod N$. Se escolhermos $\beta = 1$ obteremos $T(X)^{(n-\sigma_n).\beta} \equiv \zeta \bmod N$ com β satisfazendo (3.15): $(\zeta_2)^{\beta} \neq 1$ e N satisfazendo (3.16): $\sigma_n[N] = N$ e $N \cap Z = nZ$, portanto a condição (3.22) é satisfeita.

Se (5.6) não ocorre então $T(X)^{n-\sigma_n} \not\equiv \zeta \bmod M$ para todo $\zeta \in U_4$, em particular para $X(n)^{-n}$ teremos $T(X)^{(n-\sigma_n).\beta} \not\equiv X(n)^{-n.\beta} \bmod M$ com $\beta = 1$, logo $T(X)^{(n-\sigma_n).\beta} - X(n)^{-n.\beta} \notin M$; entretanto $j(X,X) \in Z[\zeta_4]$, então $T(X)^{n-\sigma_n} = j(X,X)^{(n-1)/2}.q^{(n-1)/4} \in Z[\zeta_4]$ e assim $T(X)^{(n-\sigma_n).\beta} - X(n)^{-n.\beta} \in Z[\zeta_4]$. Como $N \cap Z[\zeta_4] = M$ concluímos que $T(X)^{(n-\sigma_n).\beta} - X(n)^{-n.\beta} \notin N$ portanto $T(X)^{(n-\sigma_n).\beta} \not\equiv X(n)^{-n.\beta} \bmod N$. No entanto, pelo Corolário (3.14) essa congruência ocorreria se n fosse primo, logo se (5.6) não acontece n é composto. ∎

(5.7) TEOREMA: Seja $p = 2$, $k = 2$, $n \equiv 3 \bmod 4$. Se

(5.8) $j(X,X)^{(n+1)/2}.q^{(n-3)/4} \equiv \zeta \bmod nZ[\zeta_4]$ para algum $\zeta \in U_4$

então a condição (3.22) é satisfeita. Se (5.8) não ocorre então n é composto.

PROVA: Do mesmo modo que no teorema anterior, a partir de (3.9): $T(X).T(X^{-1}) = X(-1).q$ encontramos $T(X^2)^2 = q$ e através de (4.11) obtemos $T(X)^2 = j(X,X).T(X^2)$ pois $(1 + 1) \neq 0 \bmod 4$. Como $n \equiv 3 \bmod 4$ temos $n = 3 + 4.x$ com $x \in Z$, assim

$\sigma_n(\zeta_4) = (\zeta_4)^n = (\zeta_4)^3.((\zeta_4)^4)^x = (\zeta_4)^3 = (\zeta_4)^{-1}$; por outro lado $x^n = x^{-1}$ visto que x tem ordem 4. Verificamos então que $T(X)^{\sigma_n} = \sigma_n(\sum_{x=1}^{q-1} X(x).(\zeta_q)^x) = \sum_{x=1}^{q-1} X^n(x).(\zeta_q)^x = \sum_{x=1}^{q-1} X^{-1}(x).(\zeta_q)^x$ portanto $T(X)^{\sigma_n} = T(X^{-1})$ e $T(X)^{-\sigma_n} = T(X^{-1})^{-1}$; assim

$T(X)^{n-\sigma_n} = T(X)^n.T(X^{-1})^{-1} = (T(X)^n/T(X^{-1})).(T(X)/T(X)) =$

$= T(X)^{n+1}/(T(X^{-1}).T(X))$ então

(5.9) $T(X)^{n-\sigma_n} = T(X)^{n+1}/(X(-1).q)$

Por outro lado $T(X)^{n+1} = (T(X)^2)^{(n+1)/2} =$

$= j(X,X)^{(n+1)/2}.T(X^2)^{(n+1)/2}$, mas $T(X^2)^2 = q$ portanto $T(X)^{n+1} = j(X,X)^{(n+1)/2}.q^{(n+1)/4}$. Substituindo $T(X)^{n+1}$ por esse novo valor em (5.9) obtemos $T(X)^{n-\sigma_n} = (j(X,X)^{(n+1)/2}.q^{(n+1)/4})/X(-1).q$ ou equivalentemente $T(X)^{n-\sigma_n}.X(-1) = j(X,X)^{(n+1)/2}.q^{(n-3)/4}$ e então, por (5.8) obtemos $T(X)^{n-\sigma_n}.X(-1) \equiv \zeta \bmod nZ[\zeta_4]$, mas $X(-1) = 1$ ou $X(-1) = -1$ de modo que $X(-1)$ é inversível e $X(-1) = X(-1)^{-1} \in U_4$, logo $\zeta' = X(-1)^{-1}.\zeta \in U_4$ e então $T(X)^{n-\sigma_n} \equiv \zeta' \bmod nZ[\zeta_4]$. Se escolhermos $\beta = 1$ e $N = nB$, β satisfaz (3.15): $(\zeta_2)^\beta \neq 1$ e provamos na Proposição (5.2) que N satisfaz (3.16). Como $nZ[\zeta_4] \subset nB$ temos $T(X)^{(n-\sigma_n).\beta} \equiv X(-1).\zeta \bmod N$ e portanto a condição (3.22) é satisfeita.

Se a congruência (5.8) não acontece então $T(X)^{n-\sigma_n} \not\equiv \zeta \bmod nZ[\zeta_4]$ qualquer $\zeta \in U_4$; em particular se $\beta = 1$ e $\zeta = X(n)^{-n.\beta}$ obtemos $T(X)^{(n-\sigma_n).\beta} \not\equiv X(n)^{-n.\beta} \bmod nZ[\zeta_4]$, isto é, $T(X)^{(n-\sigma_n).\beta} - X(n)^{-n.\beta} \notin nZ[\zeta_4]$; contudo $j(X,X) \in nZ[\zeta_4]$ de modo que $T(X)^{(n-\sigma_n).\beta} = j(X,X)^{(n+1)/2}.q^{(n-3)/4}.X(-1) \in Z[\zeta_4]$ e isso implica em $T(X)^{(n-\sigma_n).\beta} - X(n)^{-n.\beta} \in Z[\zeta_4]$. Pela Proposição (5.2)

provamos que $nB \cap \mathbb{Z}[\zeta_4] = n\mathbb{Z}[\zeta_4]$ o que nos faz concluir que $T(X)^{(n-\sigma_n).\beta} - X(n)^{-n.\beta} \notin nB$. No entanto, se n fosse primo ocorreria a congruência, portanto se não vale a congruência (5.8) n é composto. ■

Assumindo para o restante do parágrafo $p = 2$ e $k \geqslant 3$, definiremos Soma de Jacobi Tripla $j(X,X,X)$ como um elemento de $\mathbb{Z}[\zeta_{2^k}]$ da seguinte forma:

(5.10) $j(X,X,X) = j(X,X).j(X,X^2)$

De (4.11) temos $j(X^a,X^b) = T(X^a).T(X^b)/T(X^{a+b})$ se $a + b \not\equiv 0 \bmod p^k$, assim, $j(X,X) = T(X)^2/T(X^2)$ e $j(X,X^2) = T(X).T(X^2)/T(X^3)$ visto que $3 \not\equiv 0 \bmod 2^k$ e $2 \not\equiv 0 \bmod 2^k$ para $k \geqslant 3$. Substituindo esses valores em (5.10) obteremos

(5.11) $j(X,X,X) = T(X)^3/T(X^3) = T(X)^{3-\sigma_3}$

pois $T(X^3) = \sum_{x=1}^{q-1} X^3(x).(\zeta_q)^x = \sigma_3(T(X)) = T(X)^{\sigma_3}$. Seja

(5.12) $W = \{x \in \mathbb{Z} : 1 \leqslant x \leqslant 2^k,\ x \equiv 1 \text{ ou } 3 \bmod 8\}$ e

$\overline{W} = \{x \bmod 2^k,\ x \in W\}$

As proposições que provaremos a seguir serão utilizadas no Teorema (5.17).

(5.13) PROPOSIÇÃO: $\overline{W}$ é um subgrupo de $(\mathbb{Z}/2^k\mathbb{Z})^*$ de ordem 2^{k-2}. Além disso $\sum_{x\in W} x = 2^{k-1} + 2^{2.k-3} - 2^k$.

PROVA: Para provar que $\overline{W}$ é um subgrupo de $(\mathbb{Z}/2^k\mathbb{Z})^*$, notemos primeiramente que todo elemento de $\overline{W}$ pertence a $(\mathbb{Z}/2^k\mathbb{Z})^*$; assim precisamos apenas verificar as propriedades do fechamento e inverso mul-

tiplicativo. Por definição qualquer elemento de $\overline{M}$ é côngruo a 1 ou 3 módulo 8 e é fácil observar que o produto de elementos côngruos a 1 ou 3 módulo 8 também é côngruo a 1 ou 3 módulo 8, portanto a propriedade de fechamento é satisfeita. Por outro lado o inverso de um elemento côngruo a 3 módulo 8 também é côngruo a 3 módulo 8. Obtemos então $\overline{W}$ como subgrupo de $(\mathbb{Z}/2^k\mathbb{Z})^*$. A ordem desse subgrupo é 2^{k-2} visto que para $k \geqslant 3$ existem $2^k/8$ elementos côngruos a 1 módulo 8 e outros $2^k/8$ elementos côngruos a 3 módulo 8, ou seja, o subconjunto possui $2^{k-3} + 2^{k-3}$ elementos. Para calcular $\sum_{x\in W} x$ notemos que

$$W = \{1 + 8.i : i \in \mathbb{Z},\ 0 \leqslant i \leqslant 2^{k-3} - 1\} \cup$$

$$\cup \{3 + 8.i : i \in \mathbb{Z},\ 0 \leqslant i \leqslant 2^{k-3} - 1\}$$ portanto

$$\sum_{x\in W} x = \sum_{i=0}^{2^{k-3}-1}(1 + 8.i) + \sum_{i=0}^{2^{k-3}-1}(3 + 8.i) = \sum_{i=0}^{2^{k-3}-1} 1 + \sum_{i=0}^{2^{k-3}-1} 3 + 2.\sum_{i=0}^{2^{k-3}-1} 8.i =$$

$$= 4.\sum_{i=0}^{2^{k-3}-1} 1 + 16.\sum_{i=0}^{2^{k-3}-1} i. \quad A \sum_{i=0}^{2^{k-3}-1} i$$ corresponde a soma dos 2^{k-3} primeiros termos de uma Progressão Aritmética de razão 1, logo

$$\sum_{i=0}^{2^{k-3}-1} i = ((0 + 2^{k-3} - 1).2^{k-3})/2 = 2^{2.k-7} - 2^{k-4}$$ e então

$$\sum_{x\in W} x = 2^2.2^{k-3} + 2^4.(2^{2.k-7} - 2^{k-4}) = 2^{k-1} + 2^{2.k-3} - 2^k. \quad \blacksquare$$

Como no parágrafo anterior, dado $y \in Q$, $[y]$ será o maior inteiro menor ou igual a y.

(5.14) PROPOSIÇÃO: Sejam $\alpha = \sum_{x\in W}[n.x/2^k].(\overline{\sigma}_x)^{-1}$, $\beta = \sum_{x\in W}[3.x/2^k].(\overline{\sigma}_x)^{-1}$ e $n \equiv 1$ ou $3 \bmod 8$. Então $(n - \overline{\sigma}_n).\beta = (3 - \overline{\sigma}_3).\alpha$.

PROVA: Seja $\theta = \sum_{x\in W} x.(\overline{\sigma}_x)^{-1}$. O mesmo procedimento utilizado no Lema (4.24) para obter a igualdade (4.25) pode ser aplicado aqui

resultando em:

(5.15) $(m - \sigma_m).\theta = 2^k.\sum_{y\in W}[m.y/2^k].(\sigma_y)^{-1}$ para $m \in Z$, $m \equiv 1$ ou $3 \bmod 8$

Claramente (5.15) é válida para $m = n$ e para $m = 3$, assim substituindo y por x (pois ambos percorrem W) em (5.15) obtemos $(n - \sigma_n).\theta = 2^k.\sum_{x\in W}[n.x/2^k].(\sigma_x)^{-1} = 2^k.\alpha$. e $(3 - \sigma_3).\theta = 2^k.\sum_{x\in W}[3.x/2^k].(\sigma_x)^{-1} = 2^k.\beta$. Utilizando as duas últimas igualdades encontramos $(2^k.\beta).(n - \sigma_n) = (3 - \sigma_3).\theta.(n - \sigma_n) = 2^k.(3 - \sigma_3).\alpha$. No entanto Z[G] é livre de torção pois é um anel de grupo e desse modo 2^k pode ser cancelado na igualdade acima; portanto $(n - \sigma_n).\beta = (3 - \sigma_3).\alpha$. ∎

(5.16) PROPOSIÇÃO: Se $\beta = \sum_{x\in W}[3.x/2^k].(\sigma_x)^{-1}$ e Z[G] então $(\zeta_2)^\beta \neq 1$.

PROVA: Seja $\varphi : Z[G] \longrightarrow Z$ tal que $\varphi(\sigma_x) = 1$ para todo $\sigma_x \in G$ e $\varphi(z) = z$ para $z \in Z$. φ é um homomorfismo de anéis pois dados $\sum_{x\in W} r_x.\sigma_x$, $\sum_{x\in W} s_x.\sigma_x$, $\sum_{y\in W} t_y.\sigma_y \in Z[G]$, $\varphi(\sum_{x\in W} r_x.\sigma_x + \sum_{x\in W} s_x.\sigma_x) =$ $= \varphi(\sum_{x\in W}(r_x + s_x).\sigma_x) = \sum_{x\in W}(r_x + s_x) = \sum_{x\in W} r_x + \sum_{x\in W} s_x =$ $= \varphi(\sum_{x\in W} r_x.\sigma_x) + \varphi(\sum_{x\in W} s_x.\sigma_x)$ e $\varphi(\sum_{x\in W} s_x.\sigma_x.\sum_{y\in W} t_y.\sigma_y) =$ $= \varphi(\sum_{z\in W}(\sum_{x.y=z} s_x.t_y).\sigma_z) = \sum_{z\in W}(\sum s_x.t_y) = \sum_{x\in W} s_x.\sum_{y\in W} t_y =$ $= \varphi(\sum_{x\in W} s_x.\sigma_x).\varphi(\sum_{y\in W} t_y.\sigma_y)$. Seja $\theta = \sum_{x\in W} x.(\sigma_x)^{-1}$. Da Proposição (5.14) temos $(3 - \sigma_3).\theta = 2^k.\beta$, logo $\varphi((3 - \sigma_3).\theta) = \varphi(2^k.\beta)$. Mas $\varphi((3 - \sigma_3).\theta) = (\varphi(3) - \varphi(\sigma_3)).\varphi(\sum_{x\in W} x.(\sigma_x)^{-1}) = (3 - 1).\sum_{x\in W} x$ e $\varphi(2^k.\beta) = \varphi(2^k).\varphi(\sum_{x\in W}[3.x/2^k].(\sigma_x)^{-1}) = 2^k.\sum_{x\in W}[3.x/2^k]$. Consequentemente $2.\sum_{x\in W} x = 2^k.\sum_{x\in W}[3.x/2^k]$. Já calculamos $\sum_{x\in W} x$ na Proposição (5.13) logo $\sum_{x\in W}[3.x/2^k] = (2^{k-1} + 2^{2.k-3} - 2^k)/2^{k-1} =$

$= 1 + 2^{k-2} - 2 = 2^{k-2} - 1$. $(-1)^{\beta} = (-1)^{\sum_{x\in W}[3.x/2^k].(\sigma_x)^{-1}} =$

$= \prod_{x\in W}((\sigma_x)^{-1}(-1))^{[3.x/2^k]}$. Notemos que $(\sigma_x)^{-1} \in G$, logo $(\sigma_x)^{-1}$ leva raiz 2^k-ésima da unidade em raiz 2^k-ésima de mesma ordem, entretanto a única raiz 2^k-ésima de ordem 2 é o $-1 = \zeta_2$ logo $(\sigma_x)^{-1}(-1) = -1$ para todo $x \in W$; encontramos então $(-1)^{\beta} = \prod_{x\in W}(-1)^{[3.x/2^k]} = (-1)^{\sum_{x\in W}[3.x/2^k]} = (-1)^{2^{k-2}-1}$. Observemos agora que $k \geq 3$ logo $2^{k-2}-1$ é ímpar o que implica em $(-1)^{2^{k-2}-1} = -1$ portanto $(\zeta_2)^{\beta} = (-1)^{\beta} = -1$. Como consequência β satisfaz a condição (3.15): $(\zeta_2)^{\beta} \neq 1$.

(5.17) TEOREMA: Seja $p = 2$, $k \geq 3$ e $m \equiv 1$ ou $3 \bmod 8$. Seja M um ideal de $Z[\zeta_{2^k}]$ para o qual $M \cap Z = nZ$ e $\sigma_n[M] = M$. Seja $\alpha \in Z[G]$, $\alpha = \sum_{x\in W}[n.x/2^k].(\sigma_x)^{-1}$. Se

(5.18) $j(X,X,X)^{\alpha} \equiv \zeta \bmod M$ para algum $\zeta \in U_{2^k}$

então a condição (3.22) é satisfeita. Se (5.18) não ocorre então n é composto.

PROVA: Seja $N = \{(\sum_{j=0}^{q-2} a_j.(\zeta_q)^j).q^d \; ; \; a_j \in M \; , \; d \in Z\}$. Com procedimento idêntico ao utilizado na Proposição (4.17) obtemos $N \cap Z = nZ = M$ e $\sigma_n[N] = N$, isto é, N satisfaz (3.16). De (5.11) temos $j(X,X,X) = T(X)^{3-\sigma_3}$ o que implica em $j(X,X,X)^{\alpha} = T(X)^{(3-\sigma_3).\alpha}$. No entanto provamos na Proposição (5.14) que $(n - \sigma_n).\beta = (3 - \sigma_3).\alpha$ com $\beta = \sum_{x\in W}[3.x/2^k].(\sigma_x)^{-1}$, logo $j(X,X,X)^{\alpha} = T(X)^{(3-\sigma_3).\alpha} = T(X)^{(n-\sigma_n).\beta}$. Se $j(X,X,X)^{\alpha} \equiv \zeta \bmod M$ obtemos $T(X)^{(n-\sigma_n).\beta} \equiv \zeta \bmod M$, mas $M \subset N$, portanto $T(X)^{(n-\sigma_n).\beta} \equiv \zeta \bmod N$ para algum $\zeta \in U_{2^k}$. Pela Proposição (5.16)

temos β satisfazendo (3.15): $(\zeta_2)^{\beta} \neq 1$ e já verificamos que N satisfaz (3.16) logo a condição (3.22) é satisfeita.

Se (5.18) não ocorre então $T(X)^{(n-\sigma_n^-)\cdot\beta} \not\equiv \zeta \bmod M$ qualquer $\zeta \in U_2k$, em particular para $\zeta = X(n)^{-n\cdot\beta}$ temos $T(X)^{(n-\sigma_n^-)\cdot\beta} \not\equiv X(n)^{-n\cdot\beta} \bmod M$, logo $T(X)^{(n-\sigma_n^-)\cdot\beta} - X(n)^{-n\cdot\beta} \notin M$. No entanto $j(X,X,X) \in \mathbb{Z}[\zeta_2 k]$ e os coeficientes de α são números inteiros e positivos de modo que $j(X,X,X)^{\alpha} = T(X)^{(n-\sigma_n^-)\cdot\beta} \in \mathbb{Z}[\zeta_2 k]$, portanto $T(X)^{(n-\sigma_n^-)\cdot\beta} - X(n)^{-n\cdot\beta} \in \mathbb{Z}[\zeta_2 k]$; como já vimos em (4.17) $N \cap \mathbb{Z}[\zeta_2 k] = M$ e concluímos que $T(X)^{(n-\sigma_n^-)\cdot\beta} - X(n)^{-n\cdot\beta} \notin N$, então $T(X)^{(n-\sigma_n^-)\cdot\beta} \not\equiv X(n)^{-n\cdot\beta} \bmod N$. Contudo se n fosse primo ocorreria a congruência, logo se não vale a congruência (5.18) n é composto. ∎

Provaremos a seguir algumas proposições cujos resultados serão utilizados no Teorema (5.39).

(5.19) PROPOSIÇÃO: Seja $X : F_q^* \longrightarrow U_2k$ função caracter de ordem 2^k e $\Psi = X^{2^{k-1}}$; então $T(X).T(X.\Psi) = X(4)^{-1}.T(\Psi).T(X^2)$.

PROVA: Por definição de Soma de Jacobi, $j(X,X) = \sum_{x=0}^{q-1} X(x).X(1-x)$. Como X é homomorfismo, $j(X,X) = \sum_{x=0}^{q-1} X(x-x^2)$. Sejam $y = (x-X^2) \bmod q \in F_q$, $P(W) = W^2 - W + y \in F_q[W]$ e $\Delta = (1 - 4.y) \bmod q$. Seja m(y) o número de elementos x distintos tal que $y = (x-x^2) \bmod q$. Observemos que se Δ é um quadrado módulo q, P(W) possui duas raízes distintas em F_q, isto é, existem dois valores possíveis para x em F_q para os quais $y = (x-x^2) \bmod q$, portanto $m(y) = 2$; se $\Delta \equiv 0 \bmod q$ existe um único $x \in F_q$ tal que

$(x-x^2)$ mod q = y portanto m(y) = 1; se Δ não é quadrado módulo q não existe x em F_q tal que $(x-x^2)$ mod q = y e então m(y) = 0. Se substituirmos $x - x^2$ na somatória $\sum_{x=0}^{q-1} X(x-x^2)$ por $y = (x-x^2)$ mod q, obteremos $\sum_{x=0}^{q-1} X(x-x^2) = \sum_{y=0}^{q-1} X(y).m(y)$ de modo que

(5.20) $j(X,X) = \sum_{x=0}^{q-1} X(y).m(y)$

Dada $\Psi = X^{2^{k-1}}$, $\Psi : F_q^* \longrightarrow \{1, -1\}$ pois Ψ tem ordem 2. Se $\Delta = 1 - 4.y$ é um quadrado em F_q, existe $a \in F_q$ tal que $\Psi(1-4.y) = \Psi(a^2) = (\Psi(a))^2 = 1$ visto que $\Psi(a) = 1$ ou $\Psi(a) = -1$; assim $\Psi(1-4.y) + 1 = 2 = m(y)$. Desde que $F_q^* = (F_q^*)^2 \cup g.(F_q^*)^2$ para g gerador de F_q^*, se Δ não é um quadrado módulo q então existe $a \in F_q^*$ tal que $\Delta = 1 - 4.y = g.a^2$ em F_q^* e $\Psi(1-4.y) = \Psi(g).\Psi(a^2) = -1$, logo $\Psi(1-4.y) + 1 = 0 = m(y)$. Se $\Delta \equiv 0$ mod q, $\Psi(1-4.y) = \Psi(0) = 0$, o que implica em $\Psi(1-4.y) + 1 = 1 = m(y)$. Concluímos então que para qualquer $y \in F_q$ obtemos $m(y) = 1 + \Psi(1-4.y)$ e substituindo m(y) em (5.20) encontramos $j(X,X) = \sum_{y \in F_q} X(y).(1 + \Psi(1-4.y)) = \sum_{y \in F_q} X(y) + \sum_{y \in F_q} X(y).\Psi(1-4.y)$. Observemos agora que a soma de todas as raízes 2^k-ésimas da unidade é igual a zero, logo $\sum_{y \in F_q} X(y) = 0$ visto que $X(0) = 0$ e $\sum_{y \in F_q^*} X(y)$ corresponde a várias somatórias (exatamente $(q-1)/2^k$) de todas as raízes 2^k-ésimas da unidade. A partir disso, $j(X,X) = \sum_{y \in F_q} X(y).\Psi(1-4.y)$. Seja $z \equiv 4.y$ mod q; por hipótese $(q,4) = 1$, assim quando y percorre F_q, z também percorre F_q; além disso $(4 \text{ mod } q)^{-1} \in F_q$ de modo que $\sum_{y \in F_q} X(y).\Psi(1-4.y) = \sum_{z \in F_q} X(z/4).\Psi(1-z) = X(4^{-1}).\sum_{z \in F_q} X(z).\Psi(1-z)$, mas por definição, $\sum_{z \in F_q} X(z).\Psi(1-z) = j(X,\Psi)$, portanto

(5.21) $j(X,X) = X(4)^{-1}.j(X,\Psi)$

Retomando (4.11) obtemos $j(X,\Psi) = T(X).T(\Psi)/T(X.\Psi)$ e $j(X,X) = T(X)^2/T(X^2)$, então a igualdade (5.21) é equivalente a $T(X)^2/T(X^2) = X(4)^{-1}.T(X).T(\Psi)/T(X.\Psi)$, logo $T(X).T(X.\Psi) = X(4)^{-1}.T(\Psi).T(X^2)$ e a proposição está provada. ∎

(5.22) PROPOSIÇÃO: Dada $X : F_q^* \longrightarrow U_{2^k}$ função caracter de ordem 2^k com $k > 3$ e $\Psi = X^{2^{k-1}}$ são verdadeiras as seguintes igualdades:

(5.23) $\prod_{x\in W}\sigma_x(T(X.\Psi)) = \prod_{x\in W}\sigma_x(T(X))$ e

(5.24) $\Psi^x = \Psi$ para todo $x \in W$

PROVA: De $\Psi = X^{2^{k-1}}$ obtemos $X.\Psi = X^{2^{k-1}+1}$, no entanto $k > 3$, assim $8/2^{k-1}$ e então $2^{k-1} + 1 \equiv 1 \bmod 8$; como $2^{k-1} + 1 < 2^k$ notamos que $y = 2^{k-1} + 1 \in W$ de modo que

(5.25) $X.\Psi = X^y$ para algum $y \in W$

Por outro lado, dado $y \in W$, a função $\varphi : X^x \longrightarrow X^{x.y}$ para todo $x \in W$ é bijetiva pois dados $x,x' \in W$, se $X^{x.y} = X^{x'.y}$ temos $X^{(x-x').y} = 1$, mas $(y,2) = 1$ e a ordem de X é igual a 2^k o que implica em $2^k/(x-x')$, contudo x e x' são números inteiros positivos menores que 2^k, então $2^k/(x-x')$ se e somente se $x = x'$. Para provarmos (5.23), constatamos a partir de (5.25) que $(X.\Psi)^x = X^{x.y}$, consequentemente $\prod_{x\in W}\sigma_x(T(X.\Psi)) = \prod_{x\in W}T((X.\Psi)^x) = \prod_{x\in W}T(X^{x.y})$. Como φ é bijetiva $\prod_{x\in W}T(X^{x.y}) = \prod_{x\in W}T(X^x) = \prod_{x\in W}\sigma_x(T(X))$, portanto $\prod_{x\in W}\sigma_x(T(X.\Psi)) = \prod_{x\in W}\sigma_x(T(X))$. Para verificar (5.24) notemos que $\Psi^2 = X^{2^k}$ é a função identidade e desde que todo $x \in W$ é congruo a 1 ou 3 módulo 8 é fácil observar que x é ímpar, portanto $x = 1 + 2.w$ com $w \in \mathbb{Z}$ e então $\Psi^x = \Psi.(\Psi^2)^w = \Psi$. ∎

(5.26) PROPOSIÇÃO: Seja $X : F_q^* \longrightarrow U_{2^k}$ função caracter de ordem 2^k e $\phi = X^{2^{k-3}}$, então

(5.27) $T(X)^{2.\sum_{x\in W}\sigma_x} = q^{2^{k-2}-1}.j(\phi,\phi^3)^2$

PROVA: Relembrando que $k \geqslant 3$, a demonstração será feita aplicando indução sobre k. Para $k = 3$ temos $\phi = X$ e utilizando (4.11): $j(X^a,X^b) = T(X^a).T(X^b)/T(X^{a+b})$ se $a + b \neq 0 \bmod p^k$ encontramos $j(\phi,\phi^3) = T(\phi).T(\phi^3)/T(\phi^4)$; com isso

(5.28) $q.j(\phi,\phi^3)^2 = q.(T(\phi).T(\phi^3))^2/T(\phi^4)^2$

Observemos que para $k = 3$ a ordem de $\phi = X$ é igual a 8, assim $\phi^4 = \phi^{-4}$ e a partir de (3.9): $T(X).T(X^{-1}) = X(-1).q$ temos $T(\phi^4)^2 = \phi^4(-1).q$, mas $\phi^2(-1) = 1$, portanto $T(\phi^4)^2 = q$. Substituindo esse valor em (5.28) obtemos

(5.29) $q.j(\phi,\phi^3)^2 = (T(\phi).T(\phi^3))^2$

Notemos que para $k = 3$ $W = \{1 , 3\}$, logo $T(X)^{2.\sum_{x\in W}\sigma_x} = (\sigma_1(T(X)).\sigma_3(T(X))^2 = (T(X).T(X^3))^2$; como $\phi = X$ obtemos $T(X)^{2.\sum_{x\in W}\sigma_x} = (T(\phi).T(\phi^3))^2$ e fazendo a substituição em (5.29) encontramos $q.j(\phi,\phi^3)^2 = T(X)^{2.\sum_{x\in W}\sigma_x}$ que corresponde a (5.27) para $k = 3$.

Para $k > 3$, seja $\Psi = \phi^4 = X^{2^{k-1}}$. Já provamos em (5.23) que $T(X.\Psi)^{\sum_{x\in W}\sigma_x} = \prod_{x\in W}\sigma_x(T(X.\Psi)) = \prod_{x\in W}\sigma_x(T(X)) = T(X)^{\sum_{x\in W}\sigma_x}$ logo $T(X)^{2.\sum_{x\in W}\sigma_x} = T(X)^{\sum_{x\in W}\sigma_x} . T(X.\Psi)^{\sum_{x\in W}\sigma_x}$; provamos também em (5.19): $T(X).T(X.\Psi) = X(4)^{-1}.T(\Psi).T(X^2)$; elevando a igualdade anterior a $\sum_{x\in W}\sigma_x$ encontramos

(5.30) $T(X)^{2.\sum_{x\in W}\sigma_x} = X(4)^{-\sum_{x\in W}\sigma_x} . T(\Psi)^{\sum_{x\in W}\sigma_x} . T(X^2)^{\sum_{x\in W}\sigma_x}$

Observemos no entanto que $X(4) = X(2)^2$ e

$\sigma_x(X(2)) = X^x(2)$ de modo que $X(2)^{\sum_{x\in W}\sigma_x} = X(2)^{\sum_{x\in W}x}$; utilizando (5.24): $\Psi^x = \Psi$ temos $T(\Psi)^{\sum_{x\in W}\sigma_x} = \prod_{x\in W}\sigma_x(T(\Psi)) = \prod_{x\in W}(T(\Psi^x)) = \prod_{x\in W}T(\Psi)$; como W possui 2^{k-2} elementos, $\prod_{x\in W}T(\Psi) = T(\Psi)^{2^{k-2}}$; a igualdade (5.30) pode ser então substituída por:

(5.31) $T(X)^{2.\sum_{x\in W}\sigma_x} = X(2)^{-2.\sum_{x\in W}x}.T(\Psi)^{2^{k-2}}.T(X^2)^{\sum_{x\in W}\sigma_x}$

Na prova de (5.16) obtivemos: $2.\sum_{x\in W}x = 2^k.\sum_{x\in W}[3.x/2^k]$, logo $(X(2)^{2.\sum_{x\in W}x})^{-1} = (X(2)^{2^k})^{-\sum_{x\in W}[3.x/2^k]} = 1$ pois a ordem de X é 2^k e $\sum_{x\in W}[3.x/2^k]$ é Z. A partir de (3.9) obtemos $T(\Psi).T(\Psi^{-1}) = \Psi(-1).q$ e como $\Psi = \Psi^{-1}$, $T(\Psi)^2 = \Psi(-1).q$; assim $T(\Psi)^{2^{k-2}} = (T(\Psi)^2)^{2^{k-3}} = (\Psi(-1).q)^{2^{k-3}}$, observemos contudo que $\Psi(-1)^{2^{k-3}} = 1$ pois $\Psi(-1)^{2^{k-3}} = (\Psi(-1)^2)^{2^{k-4}} = 1$ portanto $T(\Psi)^{2^{k-2}} = q^{2^{k-3}}$. A partir desse último resultado a igualdade (5.31) pode ser substituída por

(5.32) $T(X)^{2.\sum_{x\in W}\sigma_x} = q^{2^{k-3}}.T(X^2)^{\sum_{x\in W}\sigma_x}$

Relembrando que $W = \{x : 1 \leqslant x \leqslant 2^k, x \equiv 1 \text{ ou } 3 \bmod 8\}$ seja $W' = \{x : 1 \leqslant x \leqslant 2^{k-1}, x \equiv 1 \text{ ou } 3 \bmod 8\}$. É fácil observar que $W = W' \cup \{x + 2^{k-1}, x \in W'\}$. $T(X^2)^{\sum_{x\in W}\sigma_x} = \prod_{x\in W}\sigma_x(T(X^2)) = \prod_{x\in W'}T(X^{2.x}).\prod_{y\in W\setminus W'}T(X^{2.y})$. Para cada $x \in W'$ temos $y = x + 2^{k-1} \in W\setminus W'$; claramente x distintos em W se correspondem com y distintos em $W\setminus W'$, além disso $X^{2.y} = X^{2.x}.X^{2^k} = X^{2.x}$, assim $\prod_{y\in W\setminus W'}T(X^{2.y}) = \prod_{x\in W'}T(X^{2.x})$. Então $T(X^2)^{\sum_{x\in W}\sigma_x} = \prod_{x\in W}T(X^{2.x}) = \prod_{x\in W}(T(X^{2.x}))^2$ e $\prod_{x\in W}(\sigma_x(T(X^2))^2 = T(X^2)^{2.\sum_{x\in W}\sigma_x}$, portanto $T(X^2)^{\sum_{x\in W}\sigma_x} = T(X^2)^{2.\sum_{x\in W}\sigma_x}$. Substituindo essa última igualdade em (5.32) obtemos $T(X)^{2.\sum_{x\in W}\sigma_x} = q^{2^{k-3}}.T(X^2)^{2.\sum_{x\in W}\sigma_x}$, ou equivalentemente,

(5.33) $T(X^2)^{2.\sum_{x\in W}\sigma_x} = q^{-2^{k-3}}.T(X)^{2.\sum_{x\in W}\sigma_x}$

Para aplicar a hipótese de indução suponhamos que (5.27)

é válida para k-1, isto é, para $X' = X^2 : F_q^* \longrightarrow U_{2^k}$ e $\phi' = (X^2)^{2^{(k-1)-3}}$ temos $T(X')^{2.\sum_{x\in W}\sigma_x} = q^{2^{(k-1)-2}-1}.j(\phi',(\phi')^3)^2$. Notemos contudo que $\phi' = (X^2)^{2^{k-4}} = X^{2^{k-3}} = \phi$ e substituindo ϕ' por ϕ e X' por X^2 na igualdade anterior encontramos $T(X^2)^{2.\sum_{x\in W}\sigma_x} = q^{2^{k-3}-1}.j(\phi,\phi^3)^2$ e recorrendo a (5.33) obtemos $T(X)^{2.\sum_{x\in W}\sigma_x}.q^{-2^{k-3}} = q^{2^{k-3}-1}.j(\phi,\phi^3)^2$, portanto $T(X)^{2.\sum_{x\in W}\sigma_x} = q^{2^{k-2}-1}.j(\phi,\phi^3)^2$ de modo que a igualdade (5.27) é válida para k. ∎

(5.34) PROPOSIÇÃO: Seja $X : F_q^* \longrightarrow U_{2^k}$ uma função caracter de ordem 2^k com $k \geqslant 3$; além disso $\phi = X^{2^{k-3}}$, $\alpha = \sum_{x\in W}[n.x/2^k].(\sigma_x)^{-1}$ e $\beta = \sum_{x\in W}[3.x/2^k].(\sigma_x)^{-1}$. Se $n \in \mathbb{Z}_+$ com $n \equiv 5$ ou 7 mod 8 então

(5.35) $T(X)^{(n-\sigma_n)}.\beta = X(-1).j(X,X,X).j(\phi,\phi^3)^2$

PROVA: De $n \equiv 5$ ou 7 mod 8 obtemos $-n \equiv 3$ ou 1 mod 8 e dado $\theta = \sum_{x\in W} x.(\sigma_x)^{-1}$ podemos aplicar (5.15): $(m - \sigma_m).\theta = 2^k.\sum_{x\in W}[m.x/2^k].(\sigma_x)^{-1}$ para $m = -n$ obtendo

(5.36) $(-n - \sigma_{-n}).\theta = 2^k.\sum_{x\in W}[-n.x/2^k].(\sigma_x)^{-1}$

Observemos que n e x são números ímpares de modo que $n.x/2^k \notin \mathbb{Z}$; notemos também que para $w > 0$, $z < w < z+1$ temos $[w] = z$ e $[-w] = -z-1$, ou seja, $[w] + [-w] = -1$, logo $\sum_{x\in W}([-n.x/2^k] + [n.x/2^k]).(\sigma_x)^{-1} = -\sum_{x\in W}(\sigma_x)^{-1}$; por outro lado $\sum_{x\in W}(\sigma_x)^{-1} = \sum_{x\in W}\sigma_x$ e $\sum_{x\in W}[n.x/2^k].(\sigma_x)^{-1} = \alpha$ de modo que $\sum_{x\in W}[-n.x/2^k].(\sigma_x)^{-1} = -(\alpha + \sum_{x\in W}\sigma_x)$. Se substituirmos o valor acima em (5.36) obtemos $(-n - \sigma_{-n}).\theta = -2^k.(\alpha + \sum_{x\in W}\sigma_x)$. Também provamos que $(n - \sigma_n).\theta = 2^k.\alpha$ e $(3 - \sigma_3).\theta = 2^k.\beta$, assim, combinando

esses resultados com a igualdade anterior encontramos

$(n + \sigma_{-n}).\beta = (n + \sigma_{-n}).(3 - \sigma_3).\theta.2^{-k} =$

$= (3 - \sigma_3).2^k.(\alpha + \sum_{x\in W}\sigma_x).2^{-k} = (3 - \sigma_3).\alpha + (3 - \sigma_3).\sum_{x\in W}\sigma_x$ portanto $(n + \sigma_{-n}).\beta = (3 - \sigma_3).\alpha + 2.\sum_{x\in W}\sigma_x$ então

$T(X)^{(n+\sigma_{-n}).\beta} = T(X)^{(3-\sigma_3).\alpha}.T(X)^{2.\sum_{x\in W}\sigma_x}$ mas por (5.11):

$j(X,X,X) = T(X)^{(3-\sigma_3)}$, logo

(5.37) $T(X)^{(n+\sigma_{-n}).\beta} = j(X,X,X)^{\alpha}.T(X)^{2.\sum_{x\in W}\sigma_x}$

Por outro lado, como $T(X).T(X^{-1}) = X(-1).q$ temos $T(X)^{\sigma_n+\sigma_{-n}} = \sigma_n(T(X)).\sigma_{-n}(T(X)) = T(X^n).T(X^{-n}) = X^n(-1).q$, mas $X^n(-1) = X(-1)$ pois $X(-1) = 1$ ou -1 e n é ímpar, logo $T(X)^{\sigma_n+\sigma_{-n}} = X(-1).q$ e $T(X)^{(\sigma_n+\sigma_{-n}).\beta} = (X(-1).q)^{\beta}$; no entanto para todo $x \in W$, $(\sigma_x)^{-1}(X(-1)) = X(-1)$ pois $X(-1)$ é o único elemento de ordem 2 do grupo U_{2^k}, então $X(-1)^{\beta} = X(-1)^{\sum_{x\in W}[3.x/2^k]}$, mas por (5.16): $\sum_{x\in W}[3.x/2^k] = 2^{k-2} - 1$ é um número ímpar portanto $X(-1)^{\beta} = X(-1)$. Por outro lado $(\sigma_x)^{-1}(q) = q$, assim $q^{\beta} = q^{\sum_{x\in W}[3.x/2^k]} = q^{2^{k-2}-1}$; além disso $\sigma_3.\sum_{x\in W}\sigma_x = \sum_{x\in W}\sigma_3.\sigma_x = \sum_{x\in W}\sigma_x$. Desse modo

(5.38) $T(X)^{(\sigma_n+\sigma_{-n}).\beta} = X(-1).q^{2^{k-2}-1}$

Claramente a expressão (5.38) é diferente de zero e dividindo (5.37) por (5.38) encontramos $T(X)^{(n-\sigma_n).\beta} = (j(X,X,X)^{\alpha}.T(X)^{2.\sum_{x\in W}\sigma_x})/(X(-1).q^{2^{k-2}-1})$. No entanto $X(-1) = X(-1)^{-1}$ e já provamos em (5.27) que $T(X)^{2.\sum_{x\in W}\sigma_x} = q^{2^{k-2}-1}.j(\phi,\phi^3)^2$; assim $T(X)^{(n-\sigma_n).\beta} = X(-1).j(X,X,X)^{\alpha}.j(\phi,\phi^3)^2$ e a igualdade (5.35) está verificada. ∎

(5.39) TEOREMA: Seja $p = 2$, $k \geqslant 3$ e $n \equiv 5$ ou $7 \bmod 8$. Seja M ideal de $\mathbb{Z}[\zeta_{2^k}]$ para o qual $M \cap \mathbb{Z} = n\mathbb{Z}$ e $\sigma_n[M] = M$; seja $\alpha = \sum_{x \in W}[n.x/2^k].(\sigma_x)^{-1}$ e $\phi = x^{2^{k-3}}$. Se

(5.40) $j(X,X,X)^{\alpha}.j(\phi,\phi^3)^2 \equiv \zeta \bmod M$ para algum $\zeta \in U_{2^k}$

então a condição (3.22) é satisfeita. Se (5.40) não ocorre então n é composto.

PROVA: Seja $\beta = \sum_{x \in W}[3.x/2^k].(\sigma_x)^{-1}$. Provamos na Proposição (5.34) que $T(X)^{(n-\sigma_n).\beta} = X(-1).j(X,X,X)^{\alpha}.j(\phi,\phi^3)^2$. Como $X(-1) = 1$ ou -1 podemos multiplicar (5.40) por $X(-1)$ obtendo $X(-1).j(X,X,X)^{\alpha}.j(\phi,\phi^3)^2 \equiv X(-1).\zeta \bmod M$ portanto $T(X)^{(n-\sigma_n).\beta} \equiv X(-1).\zeta \bmod M$ para algum $\zeta \in U_{2^k}$. No entanto $X(-1) \in U_{2^k}$ o que implica em $\zeta' = X(-1).\zeta \in U_{2^k}$. Já provamos na Proposição (5.16) que $(-1)^{\beta} \neq 1$, ou equivalentemente, β satisfaz a condição (3.15). Basta tomarmos o ideal $N = \{(\sum_{j=0}^{q-2} a_j.(\zeta_q)^j).q^d : a_j \in M \quad (0 \leqslant j \leqslant q-2) \ , \ d \in \mathbb{Z}\}$ para o qual a condição (3.16) é satisfeita e encontramos $T(X)^{(n-\sigma_n).\beta} \equiv \zeta' \bmod N$ e portanto (3.22) é satisfeita.

Suponhamos agora que (5.40) não ocorre, isto é, $j(X,X,X)^{\alpha}.j(\phi,\phi^3)^2 \not\equiv \zeta \bmod M$ para todo $\zeta \in U_{2^k}$ e com isso $T(X)^{(n-\sigma_n).\beta} \not\equiv \zeta \bmod M$ qualquer que seja $\zeta \in U_{2^k}$; em particular para $X(n)^{-n.\beta} \in U_{2^k}$ temos $T(X)^{(n-\sigma_n).\beta} \not\equiv X(n)^{-n.\beta} \bmod M$, logo $T(X)^{(n-\sigma_n).\beta} - X(n)^{-n.\beta} \notin M$; no entanto $j(X,X,X)$ e $j(\phi,\phi^3)$ pertencem a $\mathbb{Z}[\zeta_{2^k}]$ e os coeficientes de α são números inteiros e positivos de modo que $j(X,X,X)^{\alpha}.j(\phi,\phi^3)^2.X(-1) = T(X)^{(n-\sigma_n).\beta} \in \mathbb{Z}[\zeta_{2^k}]$ portanto $T(X)^{(n-\sigma_n).\beta} - X(n)^{-n.\beta} \in \mathbb{Z}[\zeta_{2^k}]$, mas já vimos anterior-

BIBLIOGRAFIA

1. L.M. Adleman, C. Pomerance and R.S. Rumely. "On distinguishing prime numbers from composite numbers". Annals of Mathematics, v. 117 pp. 173-206, 1.983

2. G. Bachman. Introduction to p-Adic Numbers and Valuation Theory. Academic Press Inc. 1.964.

3. H. Cohen and H.W. Lenstra, Jr. "Primality Testing and Jacoby Sums". Mathematics of computation, v.42, January 1.984, pp. 297-330.

4. I.N. Herstein. Tópicos de Álgebra, Polígono, São Paulo, 1.970.

5. D.E. Knuth. The Art of Computer Programming, v. 2, Seminumerical Algorithims, 2nd ed, Addison-Wesley, Reading, Mass., 1.981

6. S. Lang. Álgebra, Addison-Wesley, Reading, Mass., 1.965.

7. H.W. Lenstra, Jr.. "Primality Testing Algorithims (after Adleman, Rumely and Williams), Sem. Bourbaki, v. 33, 1.980/ 1.981, Expose 576, pp. 243-257.

8. J.L. Nicolas. "Tests de Primalité". Expositiones Mathematicae 2, pp. 223-234, Bibliographisches Institut GA 1.984.

9. I. Niven and H.S. Zuckerman. An Introduction to the Theory of Numbers, John Wiley & Sons Inc..

10. P. Samuel. Théorie algébrique des nombres, Hermann, Paris, 1.967.

11. J.P. Serre. Cours d'Arithmétique, Presses Universitaires de France, Paris, 1.970.

12. T.M. Viswanathan. Introdução a Álgebra e Aritmética, Impa, 1.979.

13. O. Zariski and P. Samuel. Commutative Algebra, Van Nostrand Reinhold Company, 1.958.

14. L.C. Washington. Introduction to Cyclotomic Fields, Springer-Verlag, New York, 1.982.