O Lema de Hensel

No início de 2005, tive o imenso prazer e grande oportunidade de trabalhar e conviver com o professor Svetoslav Savchev. Devo dizer que esse período foi um dos períodos em que mais aprendi em minha vida, não só Matemática como ensino também. Aprendi que não basta resolver os problemas; é importante melhorar cada solução sempre, e encontrar o máximo de soluções o mais diferentes possíveis.

Nesse pequeno artigo vou compartilhar um lema que ele ensinou que é um atalho muito interessante para problemas de Teoria dos Números.

1. O lema

Lema de Hensel. *Seja p um primo ímpar, a um inteiro e n um inteiro positivo. Sejam α e β inteiros não negativos, com $\alpha > 0$.*

(i) Se a maior potência de p que divide n é p^β e a maior potência de p que divide $a-1$ é p^α (atenção, p deve dividir $a-1$! Mas note que p não precisa dividir n), então a maior potência de p que divide a^n-1 é $p^{\alpha+\beta}$.

(ii) Se n é ímpar, a maior potência de p que divide n é p^β e a maior potência de p que divide $a+1$ é p^α (as mesmas condições sobre os expoentes α e β do item (i) devem valer), então a maior potência de p que divide a^n+1 é $p^{\alpha+\beta}$.

Demonstração

Vamos demonstrar o item (i). Observe que $n = p^\beta \cdot k$, sendo que k não é múltiplo de p. Primeiro provaremos o resultado para $k = 1$, ou seja, $n = p^\beta$.

A demonstração é por indução sobre β. Para $\beta = 0$ o resultado é óbvio. Suponha que o resultado é válido para $\beta = t$, ou seja, que $a^{p^t} - 1 = p^{\alpha+t} \cdot m$, com m não divisível por p. Assim, $a^{p^t} = p^{\alpha+t} \cdot m + 1$. Elevando a p dos dois lados e utilizando binômio de Newton, obtemos

$$a^{p^{t+1}} = (p^{\alpha+t} \cdot m + 1)^p = \binom{p}{0}1^p + \binom{p}{1}1^{p-1}p^{\alpha+t}m + \binom{p}{2}1^{p-2}(p^{\alpha+t}m)^2 + \cdots + \binom{p}{p}(p^{\alpha+t}m)^p$$
$$\iff a^{p^{t+1}} - 1 = p^{\alpha+t+1}(m + p \cdot v),$$

em que v é um inteiro. Logo, como m não é divisível por p, o resultado está provado para $k = 1$.

Se $k > 1$, basta observar que

$$a^{p^\beta \cdot k} - 1 = \left(a^{p^\beta}\right)^k - 1 = (a^{p^\beta} - 1)(a^{p^\beta \cdot (k-1)} + a^{p^\beta \cdot (k-2)} + \cdots + a^{p^\beta} + 1)$$

e que, sendo $d = \text{mdc}(a^{p^\beta} - 1, a^{p^\beta \cdot (k-1)} + a^{p^\beta \cdot (k-2)} + \cdots + a^{p^\beta} + 1)$, então $a^{p^\beta} \equiv 1 \pmod{d}$ e, portanto, $a^{p^\beta \cdot (k-1)} + a^{p^\beta \cdot (k-2)} + \cdots + a^{p^\beta} + 1 \equiv \underbrace{1 + 1 + \cdots + 1}_{k \text{ uns}} \equiv k \pmod{d}$. Logo $d = \text{mdc}(a^{p^\beta} - 1, k)$. Como k não tem divisor primo p, então o fator $a^{p^\beta \cdot (k-1)} + a^{p^\beta \cdot (k-2)} + \cdots + a^{p^\beta} + 1$ não tem fator p, de modo que a maior potência de p que divide $(a^{p^\beta} - 1)(a^{p^\beta \cdot (k-1)} + a^{p^\beta \cdot (k-2)} + \cdots + a^{p^\beta} + 1) = a^{p^\beta \cdot k} - 1$ é $p^{\alpha+\beta}$. ∎

2. Aplicando o lema

O próximo problema caiu na IMO em que o Gugu ganhou medalha de ouro.

Exemplo 2.1.

Problema 6, IMO 1990. *Encontre todos os inteiros positivos n tais que $(2^n+1)/n^2$ é um número inteiro.*

Resolução

Esse tipo de problema pode ser resolvido com o seguinte procedimento:

Como resolver problemas com expoente

(1) Fatore a variável relevante em primos: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, com $p_1 < p_2 < \ldots < p_k$;

(2) Faça $i = 1$;

(3) Encontre p_i utilizando ordem;

(4) Se houver contradição, o problema acabou; caso contrário, encontre α_i utilizando o lema de Hensel;

(5) Se houver contradição, o problema acabou; caso contrário, aumente i em 1 e volte ao passo (3), ou seja, encontre o próximo primo e o próximo expoente.

Vamos aplicá-lo nesse problema.

Obviamente $n = 1$ é uma das respostas. Caso contrário, seja $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, com $p_1 < p_2 < \ldots < p_k$. Então, como n^2 divide $2^n + 1$, p_1 também o divide, ou seja,

$$2^n \equiv -1 \pmod{p_1} \implies 2^{2n} \equiv 1 \pmod{p_1}$$

Agora, seja $d_1 = \text{ord}_{p_1} 2$, isto é, o menor expoente positivo tal que $2^{d_1} \equiv 1 \pmod{p_1}$ (I). O *teorema do menor expoente* diz que a ordem de a mód m divide todo expoente t tal que $a^t \equiv 1 \pmod{m}$; em particular, divide $\phi(m)$. Assim, desse teorema, d_1 divide $2n$ e $\phi(p_1) = p_1 - 1$, ou seja, é divisor comum de $2n$ e $p_1 - 1$. Mas n só tem fatores maiores ou iguais a p_1 e $p_1 - 1$ só tem fatores menores que p_1. Assim, n e $p_1 - 1$ não tem fatores comuns, de modo que d_1 divide 2. Deste modo, de (I), $2^2 \equiv 1 \pmod{p_1} \iff p_1 | 3 \iff p_1 = 3$.

Vamos encontrar α_1. Observe que a maior potência de 3 que divide $2 + 1$ é 3. Assim, como a maior potência de 3 que divide n é 3^{α_1}, pelo lema de Hensel a maior potência de 3 que divide $2^n + 1$ é 3^{α_1+1}. Mas, como n^2 divide $2^n + 1$, então $3^{2\alpha_1}$ divide $2^n + 1$. Portanto $2\alpha_1 \leq \alpha_1 + 1 \iff \alpha_1 \leq 1 \iff \alpha_1 = 1$.

Devemos encontrar p_2 agora. Seja $d_2 = \text{ord}_{p_2} 2$. Por motivos análogos a p_1, d_2 é divisor comum de $2n$ e $p_2 - 1$. O único fator primo de n menor do que $p_2 - 1$ é $p_1 = 3$. Assim, como todos os divisores de $p_2 - 1$ são menores que p_2, concluímos que d_2 divide $2 \cdot p_1^{\alpha_1} = 2 \cdot 3^1 = 6$. Assim, $2^{d_2} \equiv 1 \pmod{p_2} \implies p_2 | 2^6 - 1$. Como $p_2 > p_1 = 3$, $p_2 = 7$.

Mas, sendo n divisível por 3, $n = 3m$, m inteiro, e $2^n + 1 = 2^{3m} + 1 = 8^m + 1 \equiv 1^m + 1 \equiv 2 \pmod{7}$, ou seja, não é possível que 7 divida $2^n + 1$. Contradição.

Podíamos ter encontrado essa contradição um pouco antes: observe que não é possível que p_2 divida $2^{p_1^{\alpha_1}} - 1$, pelo mesmo motivo do parágrafo anterior. Como provamos que p_2 divide $2^{2p_1^{\alpha_1}} - 1 = (2^{p_1^{\alpha_1}} - 1) \cdot (2^{p_1^{\alpha_1}} + 1)$, podemos concluir que p_2 divide $2^{p_1^{\alpha_1}} + 1 = 2^3 + 1$, o que não é possível.

Conseqüentemente, as únicas soluções são $n = 1$ e $n = 3$.

Uma outra aplicação é ajudar na resolução de algumas equações diofantinas com variáveis no expoente.

Exemplo 2.2.

Encontre todos os inteiros não negativos x e y tais que $7^y - 2 \cdot 3^x = 1$.

Resolução

Temos $2 \cdot 3^x = 7^y - 1$. Note que a maior potência de 3 que divide $7 - 1$ é 3. Seja 3^m a maior potência de 3 que divide y. Então, pelo lema de Hensel, a maior potência de 2 que divide $7^y - 1$ é 3^{m+1}. Logo $x \leq m + 1$. Observando ainda que, como 3^m divide y, $3^m \leq y$,

$$2 \cdot 3^{m+1} \geq 2 \cdot 3^x = 7^y - 1 \geq 7^{3^m} - 1.$$

Deste modo, sendo $t = 3^m$, temos $6t \geq 7^t - 1 \iff 7^t \leq 1 + 6t$, que é verdadeiro para $t = 0$ e $t = 1$ mas falso para $t > 1$, pois nesse caso $7^t = (6 + 1)^t > \binom{t}{0}1^t + \binom{t}{1}1^{t-1} \cdot 6 = 1 + 6t$. Notando que $t = 3^m$ e que ocorre a igualdade para $t = 1$, temos $m = 0$ e que todas as desigualdades anteriores são igualdades, isto é, $x = m + 1 = 1$ e $y = 3^m = 1$.

Exercícios

01. Prove o item (ii) do lema de Hensel.

02. Prove o teorema do menor expoente.

03. (IMO 1999, Problema 4, adaptado) Encontre todos os inteiros positivos n e primos positivos p tais que n^{p-1} divide $(p - 1)^n + 1$.

04. (IMO 2000, Problema 5) Existe um inteiro positivo n, com exatamente 2000 divisores primos distintos, tal que n divide $2^n + 1$?

05. (China 2005) Encontre todos os inteiros não negativos x, y, z e w tais que

$$2^x \cdot 3^y - 5^z \cdot 7^w = 1.$$

06. (Banco IMO 2000, proposto pelo Brasil) Encontre todas as ternas (a, m, n) de inteiros positivos tais que $a^m + 1$ divide $(a + 1)^n$.

07. (Banco IMO 1997) Seja $a > 1$ e $m > n$ inteiros positivos. Prove que se $a^m - 1$ e $a^n - 1$ têm os mesmos divisores primos então $a + 1$ é uma potência de 2.