Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 3

Carlos Gustavo Moreira

Aula 17

Famílias especiais de primos

0.1 Primos Gêmeos e Primos de Sophie Germain

Dizemos que p e q são *primos gêmeos* se p e q são primos e $|p-q| = 2$. Conjetura-se, mas não se sabe demonstrar, que existem infinitos pares de primos gêmeos. São conhecidos pares de primos gêmeos bastante grandes, como $65516468355 \cdot 2^{333333} \pm 1$, que têm 100355 dígitos cada. Brun, por outro lado, provou em [2] que primos gêmeos são escassos no seguinte sentido: se

$$\pi_2(x) = \#\{p \leq x \mid \ p \text{ e } p+2 \text{ são primos}\}$$

é o número de pares de primos gêmeos até x então

$$\pi_2(x) = O\left(\frac{x(\log\log x)^2}{(\log x)^2}\right).$$

Em particular, isto implica que

$$\sum_{p \text{ primo gêmeo}} \frac{1}{p} < +\infty,$$

enquanto sabemos que a soma sobre todos os primos $\sum_{p \text{ primo}} \frac{1}{p}$ diverge. Brun provou posteriormente em [3] que

$$\pi_2(x) < \frac{100x}{(\log x)^2}$$

para x suficientemente grande. Acredita-se, mas não se sabe demonstrar, que $\pi_2(x)$ seja assintótico a $Cx/(\log x)^2$ para alguma constante positiva C. Deixamos como exercício provar a seguinte caracterização de primos gêmeos devida a Clement. Seja $n \geq 2$; os inteiros n e $n+2$ são ambos primos se, e somente se,

$$4((n-1)!+1) + n \equiv 0 \pmod{n(n+2)}.$$

Os primos p para os quais $2p+1$ é primo são chamados de *primos de Sophie Germain*. Este nome é usado porque Sophie Germain provou o chamado primeiro caso do Último teorema de Fermat (demonstrado completamente por Wiles e Taylor) para primos p desta forma.

Proposição 1 (Sophie Germain). *Se p e $2p+1$ são primos com $p > 2$, então não existem inteiros x, y, z com* $\text{mdc}(x, y, z) = 1$ *e $p \nmid xyz$ tais que $x^p + y^p + z^p = 0$.*

Demonstração. Observe inicialmente que $2p + 1 \mid xyz$: caso contrário, pelo pequeno teorema de Fermat, $x^{2p} \equiv 1 \pmod{2p+1}$, o que equivale a $(x^p-1)(x^p+1) \equiv 0 \pmod{2p+1}$. Assim, temos que $x^p \equiv \pm 1 \pmod{2p+1}$ e analogamente $y^p \equiv \pm 1 \pmod{2p+1}$ e $z^p \equiv \pm 1 \pmod{2p+1}$. Mas $x^p+y^p+z^p \equiv \pm 1 \pm 1 \pm 1 \not\equiv 0 \pmod{2p+1}$, um absurdo.

Por outro lado, temos

$$(-x)^p = (y+z)(y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1})$$

Vamos mostrar que os dois fatores da direita são primos entre si. Se q é um primo que divide ambos os termos, então $y \equiv -z \pmod{q}$ e portanto $0 \equiv y^{p-1} - y^{p-2}z + \cdots + z^{p-1} \equiv py^{p-1} \pmod{q}$; temos $q \neq p$ pois $q \mid x$, assim $q \mid py^{p-1} \implies q \mid y$, mas então $z \equiv -y \equiv 0 \pmod{q}$ e q dividiria simultaneamente x, y, z, contrariando a hipótese $\text{mdc}(x, y, z) = 1$. Assim, pela fatoração única em primos existem inteiros a, d tais que

$$a^p = y + z \qquad \text{e} \qquad d^p = y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1}$$

e analogamente

$$b^p = x + z \qquad \text{e} \qquad e^p = x^{p-1} - x^{p-2}z + \cdots - xz^{p-2} + z^{p-1}$$
$$c^p = x + y \qquad \text{e} \qquad f^p = x^{p-1} - x^{p-2}y + \cdots - xy^{p-2} + y^{p-1}$$

para b, c, e, f inteiros.

Como $2p+1 \mid xyz$, podemos supor sem perda de generalidade que $2p+1 \mid x$. Assim, de $2x = b^p + c^p - a^p$, temos que $2p + 1 \mid b^p + c^p - a^p$ e o mesmo argumento no início da demonstração mostra que $2p + 1 \mid abc$ também. Mas se $2p+1 \mid b = x+z$ ou $2p+1 \mid c = x+y$, como $2p+1 \mid x$ e $x^p+y^p+z^p = 0$ teríamos que $2p + 1 \mid \text{mdc}(x, y, z) = 1$, um absurdo. Por outro lado, temos $f^p \equiv y^{p-1} \pmod{2p+1}$ e se $2p + 1 \mid a$, então $2p + 1 \nmid d$ e $y \equiv -z \pmod{2p+1} \implies d^p \equiv py^{p-1} \pmod{2p+1}$. Assim, $2p + 1 \mid f$, pois caso contrário teríamos $\pm p \equiv pf^p \equiv py^{p-1} \equiv d^p \equiv \pm 1 \pmod{2p+1}$, um absurdo. Mas neste caso, $2p + 1 \mid z$ também, o que é impossível já que $\text{mdc}(x, y, z) = 1$, completando a prova. □

Alguns primos de Sophie Germain bastante grandes são conhecidos, como $183027 \cdot 2^{265440} - 1$, que tem 79911 dígitos. Sabe-se também que se $\pi_{\text{SG}}(x)$ denota o número de primos de Sophie Germain menores do que x então existe C tal que para todo x

$$\pi_{\text{SG}}(x) < C\frac{x}{(\log x)^2}.$$

Acredita-se que $\pi_{\text{SG}}(x)$ seja assintótico a $cx/(\log x)^2$ para algum $c > 0$, mas não se sabe demonstrar sequer que existem infinitos primos de Sophie Germain.

Em geral, dados a, b, c números inteiros positivos, dois a dois primos entre si e com exatamente um de tais números par, denotamos por $\pi_{a,b,c}(x)$ a quantidade de pares de números primos (p, q) que satisfazem a condição $aq-bp = c$ com $p \leq x$. Hardy e Littlewood conjecturaram em [4] a seguinte estimativa assintótica para $\pi_{a,b,c}(x)$:

Conjectura 2 (Hardy, Littlewood)**.**

$$\pi_{a,b,c}(x) \sim \frac{2C}{a}\frac{x}{(\log x)^2}\prod_{\substack{p|abc\\ p\ primo>2}}\left(\frac{p-1}{p-2}\right),$$

onde $C = \prod_{\substack{p\ primo\\ p>2}}\left(1-\frac{1}{(p-1)^2}\right)$.

Em particular, se $a=1$, $b=1$ e $c=2$ temos que $\pi_{1,1,2}=\pi_2$, e se $a=1$, $b=2$ e $c=1$ temos que $\pi_{1,2,1}(x)$ é o número de primos de Sophie Germain menores do que ou iguais a x.

Fermat conjecturou que todo número da forma $F_n = 2^{2^n}+1$ fosse primo e verificou a conjectura para $n \leq 4$. Quando F_n é primo dizemos que F_n é um *primo de Fermat*. Gauss relaconou os primos de Fermat com um problema clássico de Geometria, provando que é possível construir exatamente um polígono regular de n lados com régua e compasso se, e somente se, n é da forma $2^k p_1 p_2 \dots p_r$, onde k é natural e $p_1 < p_2 < \cdots < p_r$ são primos de Fermat. Isso equivale a dizer que $\cos(2\pi/n)$ pode ser escrito a partir dos inteiros usando apenas raízes quadradas. Temos, por exemplo $\cos(2\pi/3) = -\frac{1}{2}, \cos(2\pi/5) = \frac{\sqrt{5}-1}{4}$ e $\cos(2\pi/17) =$

$$= \frac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}}{16}.$$

Observe que 2^n+1 (e em geral a^n+1 com $a \geq 2$) *não* é primo se n não é uma potência de 2: se p é um fator primo ímpar de n, podemos escrever $a^n+1 = b^p+1 = (b+1)(b^{p-1}-b^{p-2}+\cdots+b^2-b+1)$ onde $b=a^{n/p}$. Euler mostraria mais tarde que F_5 não é primo (temos $F_5 = 4294967297 = 641 \cdot 6700417$) e já se demonstrou que F_n é composto para vários outros valores de n; nenhum outro primo da forma $F_n = 2^{2^n}+1$ é conhecido. Também não se sabe se existe algum outro primo de Fermat, ou se só há um número finito de primos de Fermat. Consequentemente, o maior natural ímpar n para o qual se sabe que é possível construir com régua e compasso um polígono regular de n lados é $n = F_0F_1F_2F_3F_4 = 4294967295$.

Até outubro de 2011 o menor número de Fermat que se desconhece se é primo ou composto é F_{33}, mas se conhecem muitos primos (alguns bastante grandes) da forma $a^{2^n}+1$, que são conhecidos como *primos de Fermat generalizados*. O teste a seguir mostra como testar eficientemente a primalidade de F_n.

Proposição 3 (Teste de Pépin)**.** *Seja* $F_n = 2^{2^n}+1$*;* F_n *é primo se, e somente se,* $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

Demonstração. Se $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ então $3^{F_n-1} \equiv 1 \pmod{F_n}$. Assim, $\mathrm{ord}_{F_n} 3 \mid F_n-1$ e $\mathrm{ord}_{F_n} 3 \nmid (F_n-1)/2$, donde, como F_n-1 é uma potência de 2, $\mathrm{ord}_{F_n} 3 = F_n-1$. Como $\mathrm{ord}_{F_n} 3 \leq \varphi(F_n)$, segue que $\varphi(F_n) \geq F_n-1$, e portanto F_n é primo. Por outro lado, se F_n é primo então pelo critério de Euler e a lei de reciprocidade quadrática temos

$$3^{(F_n-1)/2} \equiv \left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1 \pmod{F_n}$$

□

1 Primos de Mersenne

Em novembro de 2013, os dez maiores primos conhecidos são da forma M_p=$2^p - 1$ para p = 57885161, 43112609, 42643801, 37156667, 32582657, 30402457, 25964951, 24036583, 20996011, 13466917. Estes são os únicos primos conhecidos com mais de 4000000 de dígitos.

Primos da forma $2^p - 1$, com p primo, têm sido estudados há séculos e são conhecidos como *primos de Mersenne*; não é difícil demonstrar que $2^p - 1$ só pode ser primo quando p é primo. Parte do interesse em primos de Mersenne deve-se à sua estreita ligação com números perfeitos. Um número perfeito é um inteiro positivo que é igual à soma de seus divisores próprios (como $6 = 1+2+3$ e $28 = 1+2+4+7+14$); os números perfeitos pares são precisamente os números da forma $2^{p-1}(2^p - 1)$ onde $2^p - 1$ é primo (um primo de Mersenne).

Talvez o primeiro resultado não trivial sobre primos de Mersenne seja devido a Hudalricus Regius que em 1536 mostrou que $2^p - 1$ não precisa ser primo sempre que p for primo: $2^{11} - 1 = 2047 = 23 \cdot 89$. Em 1603, Pietro Cataldi tinha corretamente verificado a primalidade de $2^{17} - 1$ e $2^{19} - 1$ e afirmou (incorretamente) que $2^p - 1$ também era primo para p = 23, 29, 31 e 37. Em 1640, Fermat mostrou que $2^{23} - 1$ e $2^{37} - 1$ são compostos. Em 1644, o monge Marin Mersenne (1588-1648) afirmou por sua vez (também incorretamente) que $2^p - 1$ era primo para

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 \text{ e } 257$$

e composto para os demais valores de $p \leq 257$. Esta afirmação demoraria séculos para ser completamente corrigida.

Em 1738, Euler mostrou que $2^{29} - 1$ é composto e em 1750, verificou que $2^{31} - 1$ é primo. Lucas desenvolveu um algoritmo para testar a primalidade de números de Mersenne e em 1876 verificou que $2^{127} - 1$ é primo; este número permaneceria por muito tempo como o maior primo conhecido (ver [6]). Só em 1947 a lista dos primos até 257 foi varrida: os valores de p nesta faixa para os quais $2^p - 1$ é primo são

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 \text{ e } 127.$$

O algoritmo de Lucas foi posteriormente melhorado por Lehmer para dar o seguinte critério: sejam $S_0 = 4$, $S_1 = 4^2 - 2 = 14$, ..., $S_{k+1} = S_k^2 - 2$; dado $p > 2$, $2^p - 1$ é primo se e somente se S_{p-2} é múltiplo de $2^p - 1$. Esta sequência cresce muito rápido, mas basta fazer as contas módulo $2^p - 1$: temos assim o chamado critério de Lucas-Lehmer (ver [5]).

Em 1951, computadores eletrônicos começaram a ser usados para procurar grandes números primos. Desde então foram encontrados os seguintes valores de p para os quais M_p é primo:

$$521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937,$$
$$21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433,$$
$$1257787, 1398269, 2976221, 3021377, 6972593, 13466917,$$
$$20996011, 24036583, 25964951, 30402457, 32582657,$$
$$37156667, 42643801, 43112609, 57885161.$$

Em todos os casos foi usado o critério de Lucas-Lehmer. Os últimos doze foram encontrados com a ajuda de computadores pessoais: se você tem um computador você também pode participar da busca do próximo número de Mersenne (veja as instruções em `www.mersenne.org`).

Note que um número de Mersenne M_p é escrito na base 2 como $111\ldots111$, com p dígitos. Uma generalização natural seriam os números escritos como $111\ldots111$ em outra base, isto é, números da forma $(B^p-1)/(B-1)$, onde B é a base. É fácil ver que um tal número só pode ser primo se p for primo. No caso $B=10$ estes números são conhecidos como *repunits*. Não se conhece um critério análogo ao de Lucas-Lehmer para testar a primalidade de números deste tipo quando $B>2$. O maior primo conhecido desta forma é $(28839^{8317}-1)/28838$, que tem 37090 dígitos. Os únicos repunits (comprovadamente) primos conhecidos são para $p=2,19,23,317,1031$. Recentemente (entre 1999 e 2007), foram descobertos os seguintes valores de p para os quais os repunits correspondentes são *provavelmente* primos, i.e., passam por diversos testes probabilísticos de primalidade: 49081, 86453, 109297 e 270343. De acordo com os testes já realizados, qualquer outro repunit primo deve ter mais de 400000 dígitos.

Um número de Mersenne é um número da forma $M_p=2^p-1$. Os maiores números primos conhecidos atualmente são primos de Mersenne. Uma tabela contendo os recordes atuais encontra-se no final deste capítulo. O critério de Lucas-Lehmer, que apresentaremos nesta seção, é um dos fatores para que isso ocorra pois fornece um teste de primalidade bastante rápido para números de Mersenne. Vejamos primeiramente que 2^p-1 só tem chance de ser primo quando p é primo.

Proposição 4. *Se 2^n-1 é primo então n é primo.*

Demonstração. Se $n=ab$ com $a,b\geq 2$ então $1<2^a-1<2^n-1$ e $2^n-1=2^{ab}-1=(2^a)^b-1\equiv 1^b-1=0 \pmod{2^a-1}$ e 2^n-1 é composto. □

Por outro lado, não se sabe demonstrar nem que existam infinitos primos de Mersenne nem que existem infinitos primos p para os quais M_p é composto. conjectura-se, entretanto, que existam infinitos primos p para os quais M_p é primo e que, se p_n é o n-ésimo primo deste tipo, temos

$$0<A<\frac{\log p_n}{n}<B<+\infty$$

para constantes A e B. Existem algumas conjecturas mais precisas quanto ao valor de

$$\lim_{n\to\infty}\sqrt[n]{p_n};$$

Eberhart conjectura que este limite exista e seja igual a 3/2; Wagstaff por outro lado conjectura que o limite seja

$$2^{e^{-\gamma}}\approx 1,4757613971$$

onde γ é a já mencionada constante de Euler-Mascheroni.

Primos de Mersenne são interessantes também por causa de *números perfeitos*. Um inteiro positivo n é dito *perfeito* se $\sigma(n)=2n$, onde $\sigma(n)$ é a soma dos

divisores de n. Os primeiros números perfeitos são 6, 28 e 496. Nosso próximo resultado caracteriza os números perfeitos pares.

Proposição 5. *Se M_p é um primo de Mersenne então $2^{p-1}M_p$ é perfeito. Além disso, todo número perfeito par é da forma $2^{p-1}M_p$ para algum primo p, sendo M_p um primo de Mersenne.*

Demonstração. Se M_p é primo então

$$\sigma(2^{p-1}M_p) = \sigma(2^{p-1}) \cdot \sigma(M_p) = (2^p - 1)(M_p + 1) = 2 \cdot 2^{p-1}M_p.$$

Por outro lado seja $n = 2^k b$, com $k > 0$ e b ímpar, um número perfeito par. Temos $\sigma(n) = 2n = \sigma(2^k)\sigma(b)$ donde $2^{k+1}b = (2^{k+1}-1)\sigma(b)$. Como $\text{mdc}(2^{k+1}-1, 2^{k+1}) = 1$, temos $b = (2^{k+1} - 1)c$ para algum inteiro c e assim $\sigma(b) = 2^{k+1}c$. Mas $1, 2^{k+1} - 1, c, b$ são divisores de $b = (2^{k+1} - 1)c$; se $c > 1$ então $\sigma(b) = 2^{k+1}c \geq 1 + 2^{k+1} - 1 + b$, o que implica $c \geq 2^{k+1}$, mas neste caso $\sigma(b) = 2^{k+1}c \geq 1 + 2^{k+1} - 1 + b + c$, um absurdo. Logo $c = 1$ e $b = 2^{k+1} - 1$ é primo pois $\sigma(b) = 2^{k+1}$. Pela proposição 4, $p = k + 1$ é primo, $b = M_p$ e $n = 2^{p-1}M_p$. □

Por outro lado, um dos problemas em aberto mais antigos da Matemática é o da existência de números perfeitos ímpares. Sabe-se apenas que um número perfeito ímpar, se existir, deve ser muito grande (mais de 300 dígitos) e satisfazer simultaneamente várias condições complicadas.

Conjectura 6. *Não existe nenhum número perfeito ímpar.*

Nosso próximo resultado é o critério de Lucas-Lehmer, a base dos algoritmos que testam para grandes valores de p se $2^p - 1$ é ou não primo:

Teorema 7. *Seja S_k a sequência definida por $S_0 = 4$, $S_{k+1} = S_k^2 - 2$ para todo natural k. Seja $n > 2$; $M_n = 2^n - 1$ é primo se, e somente se, S_{n-2} é múltiplo de M_n.*

Demonstração. Observemos inicialmente que

$$S_n = (2 + \sqrt{3})^{2^n} + (2 - \sqrt{3})^{2^n}$$

para todo natural n. A demonstração por indução é simples: claramente $S_0 = 4 = (2 + \sqrt{3})^{2^0} + (2 - \sqrt{3})^{2^0}$ e

$$\begin{aligned} S_{k+1} = S_k^2 - 2 &= ((2 + \sqrt{3})^{2^k} + (2 - \sqrt{3})^{2^k})^2 - 2 \\ &= ((2 + \sqrt{3})^{2^k})^2 + 2 \cdot (2 + \sqrt{3})^{2^k} \cdot (2 - \sqrt{3})^{2^k} + ((2 - \sqrt{3})^{2^k})^2 - 2 \\ &= (2 + \sqrt{3})^{2^{k+1}} + (2 - \sqrt{3})^{2^{k+1}}. \end{aligned}$$

Suponha por absurdo que $M_n \mid (2 + \sqrt{3})^{2^{n-2}} + (2 - \sqrt{3})^{2^{n-2}}$ e que M_n seja composto, com um fator primo q com $q^2 \leq M_n$. Teremos $(2 + \sqrt{3})^{2^{n-2}} + (2 - \sqrt{3})^{2^{n-2}} \equiv 0 \pmod{q}$ donde, no grupo multiplicativo $G = (\mathbb{Z}[\sqrt{3}]/(q))^\times$ dos elementos invertíveis do anel $\mathbb{Z}[\sqrt{3}]/(q)$, temos $(2 + \sqrt{3})^{2^{n-2}} = -(2 - \sqrt{3})^{2^{n-2}}$. Como $2 - \sqrt{3} = (2 + \sqrt{3})^{-1}$ esta equação pode ser reescrita como $(2 + \sqrt{3})^{2^{n-1}} =$

-1 (ainda em G), o que significa que a ordem de $2+\sqrt{3}$ em G é exatamente 2^n. Isto é um absurdo, pois o número de elementos de G é no máximo $q^2-1 < 2^n$. Fica portanto demonstrado que se S_{n-2} é múltiplo de M_n então M_n é primo.

Suponha agora M_n primo, $n > 2$. Lembramos que neste caso n é primo. Basta provar que, em $\mathbb{Z}[\sqrt{3}]$, M_n divide $S_{n-2} = (2+\sqrt{3})^{2^{n-2}} + (2-\sqrt{3})^{2^{n-2}}$, pois neste caso S_{n-2}/M_n será um inteiro algébrico racional, portanto inteiro. Assim, devemos mostrar que

$$\begin{aligned} &(2+\sqrt{3})^{2^{n-2}} \equiv -(2-\sqrt{3})^{2^{n-2}} \pmod{M_n} \\ \iff &(2+\sqrt{3})^{2^{n-1}} \equiv -1 \pmod{M_n} \end{aligned}$$

utilizando novamente o fato que $(2+\sqrt{3})(2-\sqrt{3}) = 1$. Note ainda que $2+\sqrt{3} = (1+\sqrt{3})^2/2$ e que 2 é invertível módulo M_n, logo temos que provar que

$$(1+\sqrt{3})^{M_n+1} \equiv -2^{2^{n-1}} \pmod{M_n}$$

Como M_n é primo, temos

$$\begin{aligned} (1+\sqrt{3})^{M_n} &\equiv 1 + (\sqrt{3})^{M_n} \equiv 1 + 3^{(M_n-1)/2}\sqrt{3} \\ &\equiv 1 + \left(\frac{3}{M_n}\right)\sqrt{3} \equiv 1 - \sqrt{3} \pmod{M_n} \end{aligned}$$

já que por reciprocidade quadrática temos $\left(\frac{3}{M_n}\right) = -\left(\frac{M_n}{3}\right) = -\left(\frac{-2}{3}\right) = -1$. Substituindo na expressão acima, devemos agora provar que

$$(1-\sqrt{3})(1+\sqrt{3}) \equiv -2^{2^{n-1}} \pmod{M_n} \iff 2^{2^{n-1}-1} \equiv 1 \pmod{M_n}$$

Como n é primo, $2^{n-1}-1$ é um múltiplo de n pelo pequeno teorema de Fermat. Porém, como $2^n \equiv 1 \pmod{M_n}$, isto implica que $2^{2^{n-1}-1} \equiv 1 \pmod{M_n}$ também, o que encerra a prova. □

Pretendemos falar mais sobre o critério de Lucas-Lehmer nas próximas aulas.

Mesmo quando M_p não é primo, podemos garantir que seus fatores primos serão de certas formas especiais. Isto é muito útil quando procuramos primos de Mersenne pois podemos eliminar alguns expoentes encontrando fatores primos de M_p. Isto também pode ser útil para conjecturarmos quanto à "probabilidade" de M_p ser primo, ou, mais precisamente, quanto à distribuição dos primos de Mersenne.

Proposição 8. *Sejam $p > 2$ e q primos com q um divisor de M_p. Então $q \equiv 1 \pmod{p}$ e $q \equiv \pm 1 \pmod{8}$.*

Demonstração. Se q divide M_p então $2^p \equiv 1 \pmod{q}$, o que significa que a ordem de 2 módulo q é p (pois p é primo). Isto significa que p é um divisor de $q-1$, ou seja, que $q \equiv 1 \pmod{p}$. Por outro lado, $2 \equiv 2^{p+1} = (2^{(p+1)/2})^2 \pmod{q}$, donde $\left(\frac{2}{q}\right) = 1$, o que significa que $q \equiv \pm 1 \pmod{8}$. □

Os vários valores de p para os quais a primalidade de M_p foi testada sugerem que para a ampla maioria dos valores de p, M_p *não* é primo. Isto é apenas uma conjectura: não se sabe demonstrar sequer que existem infinitos primos p para os quais M_p seja composto. Vamos agora ver uma proposição que serve para garantir que para certos valores especiais de p, alguns muito grandes, M_p *não* é primo.

Proposição 9. *Seja p primo, $p \equiv 3 \pmod 4$. Então $2p+1$ é primo (i.e. p é primo de Sophie Germain) se, e somente se, $2p+1$ divide M_p.*

Demonstração. Se $q = 2p+1$ é primo então $M_p = 2^p - 1 = 2^{(q-1)/2} - 1 \equiv \left(\frac{2}{q}\right) - 1 \pmod q$. Mas $p \equiv 3 \pmod 4$ significa que $q \equiv 7 \pmod 8$, donde $\left(\frac{2}{q}\right) = 1$. Assim, $M_p \equiv 0 \pmod q$, o que demonstra uma das implicações da proposição.

Por outro lado, se $2p+1$ não é primo, ele tem fatores primos r com $r \not\equiv 1 \pmod p$ (pois $r < p$). Se $2p+1$ dividisse M_p, r seria um fator primo de M_p, contrariando a proposição anterior. □

Problemas Propostos

Problema 10. *Prove que se n e d são inteiros maiores que 1 com $\mathrm{mcd}(n, d!) = 1$, tem-se que n e $n+d$ são primos se, e somente se, $d!d((n-1)!+1)+n(d!-1) \equiv 0 \pmod{n(n+d)}$.*

Problema 11. *Sierpinski provou que existem infinitos números naturais ímpares k (os números de Sierpinski tais que $k \cdot 2^n + 1$ é composto para todo natural n.*

Prove que 78557 é um número de Sierpinski, e que existem infinitos números de Sierpinski a partir das congruências

$$78557 \cdot 2^0 + 1 \equiv 0 \pmod 3$$

$$78557 \cdot 2^1 + 1 \equiv 0 \pmod 5$$

$$78557 \cdot 2^7 + 1 \equiv 0 \pmod 7$$

$$78557 \cdot 2^{11} + 1 \equiv 0 \pmod{13}$$

$$78557 \cdot 2^3 + 1 \equiv 78557 \cdot 2^{39} + 1 \equiv 0 \pmod{73}$$

$$78557 \cdot 2^{15} + 1 \equiv 0 \pmod{19}$$

$$78557 \cdot 2^{27} + 1 \equiv 0 \pmod{37}.$$

Problema 12. *Mostrar que se p é um número primo, então $p^p - 1$ tem um fator primo que é congruente a 1 módulo p.*

Problema 13. *Dados dois números reais α e β tais que $0 \leq \alpha < \beta \leq 1$, demonstrar que existe um número natural m tal que*

$$\alpha < \frac{\varphi(m)}{m} < \beta.$$

Problema 14. *Seja m um inteiro positivo. Dizemos que um inteiro $m \geq 1$ é "superabundante" se*

$$\forall k \in \{1, 2, \ldots, m-1\} \qquad \frac{\sigma(m)}{m} > \frac{\sigma(k)}{k}.$$

Demonstrar que existe um número infinito de números superabundantes.

Problema 15. *Demonstrar que $d(n) < 2\sqrt{n}$.*

Problema 16. *Demonstrar que*

$$\frac{\sigma(n)}{d(n)} \geq \sqrt{n}.$$

Problema 17. *Encontrar todos os valores de n para os quais $\varphi(n) \mid n$.*

Problema 18. *Dois números a e b são* amigáveis *se $\sigma(a) = b$ e $\sigma(b) = a$. Por exemplo* 1184 *e* 1210 *são amigáveis (verificar!). Encontrar outra dupla de números amigáveis.*

Problema 19. *Demonstrar que $m \mid \sigma(mn-1)$ para todo n se, e só se, $m =$* 2, 3, 4, 6, 8, 12 *ou* 24.

Problema 20. *Demonstrar que*

$$\frac{\sigma(n!)}{n!} > 1 + \frac{1}{2} + \cdots + \frac{1}{n}.$$

Problema 21. *Demonstrar que existem infinitos números naturais n para os quais $\sigma(x) = n$ não tem solução.*

Problema 22. *Demonstrar que para todo $m > 1$*

$$\left| \sum_{k=1}^{m} \frac{\mu(k)}{k} \right| < \frac{2}{3}.$$

Problema 23 (IMO1998)**.** *Para cada inteiro positivo n, $d(n)$ denota o número de divisores de n. Determine todos os inteiros positivos k tais que $d(n^2) = kd(n)$ para algum n.*

Problema 24. *Se n é composto, mostre que $\varphi(n) \leq n - \sqrt{n}$.*

Problema 25. *Determinar todos os números inteiros positivos n tais que $n = d(n)^2$.*

Problema 26. *Mostrar que $\varphi(n) + \sigma(n) \geq 2n$ para todo inteiro positivo n.*

Problema 27. *Seja $f : \mathbb{N}^+ \to \mathbb{R}^+$ uma função multiplicativa e crescente.*

(a) Prove que, para todo inteiro $M > 1$ e todo inteiro positivo n,

$$f(M^{n+1} - 1) \geq f(M^n - 1)f(M) \text{ e } f(M^{n+1} + 1) \leq f(M^n + 1)f(M).$$

Conclua que

$$\lim_{n \to \infty} \sqrt[n]{f(M^n)} = f(M).$$

(b) *Utilize o item anterior para M potência de primo para concluir que* $f(p^k) = f(p)^k$ *para todo primo* p.

(c) *Conclua que* f *é totalmente multiplicativa, e portanto existe* $\alpha > 0$ *tal que* $f(n) = n^\alpha$ *para todo inteiro positivo* n.

Problema 28. *Dadas duas funções* $f, g : \mathbb{N}_{>0} \to \mathbb{C}$, *definimos o produto de Dirichlet (ou convolução de Dirichlet)* $f * g : \mathbb{N}_{>0} \to \mathbb{C}$ *de* f *e* g *por*

$$f * g(n) \stackrel{\text{def}}{=} \sum_{d|n} f(d) g\Big(\frac{n}{d}\Big) = \sum_{d_1 d_2 = n} f(d_1) g(d_2).$$

(a) *Prove que, se* $s \in \mathbb{R}$ *(ou* $s \in \mathbb{C}$*) e as séries* $\sum_{n\geq 1} \frac{f(n)}{n^s}$ *e* $\sum_{n\geq 1} \frac{g(n)}{n^s}$ *convergem absolutamente então*

$$\sum_{n\geq 1} \frac{f(n)}{n^s} \cdot \sum_{n\geq 1} \frac{g(n)}{n^s} = \sum_{n\geq 1} \frac{f * g(n)}{n^s}.$$

(b) *Prove que, para quaisquer funções* $f, g, h : \mathbb{N}_{>0} \to \mathbb{C}$, *temos* $f * g = g * f$ *e* $f * (g * h) = (f * g) * h$ *(isto é, o produto de Dirichlet é comutativo e associativo), e que a função* $I : \mathbb{N}_{>0} \to \mathbb{C}$ *dada por* $I(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n > 1 \end{cases}$ *é o elemento neutro do produto* $*$, *i.e.,* $I * f = f * I = f$, $\forall f : \mathbb{N}_{>0} \to \mathbb{C}$.

(c) *Prove que se* f *e* g *são multiplicativas então* $f * g$ *é multiplicativa.*

(d) *Prove que, se* $f : \mathbb{N}_{>0} \to \mathbb{C}$ *é tal que* $f(1) \neq 0$, *então existe uma única função* $f^{(-1)} : \mathbb{N}_{>0} \to \mathbb{C}$ *tal que* $f * f^{(-1)} = f^{(-1)} * f = I$, *a qual é dada recursivamente por* $f^{(-1)}(1) = 1/f(1)$ *e, para* $n > 1$,

$$f^{(-1)}(n) = -\frac{1}{f(1)} \sum_{d|n, d<n} f\Big(\frac{n}{d}\Big) f^{(-1)}(d).$$

(e) *Prove que, se* f *é multiplicativa, então a função* $f^{(-1)}$ *definida no item anterior também é multiplicativa.*

Dicas e Soluções

Em breve

Referências

[1] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha, E. Tengan - Teoria dos Números - um passeio com primos e outros números familiares pelo mundo inteiro, Projeto Euclides, IMPA, 2010.

[2] V. Brun, *La série* $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\ldots$ *où les dénominateurs sont nombres premiers jumeaux est convergente ou finie*, Bull. Sci. Math., (2) 43 (1919), 100-104, 124-128.

[3] V. Brun, *Le crible d'Eratosthène et le théorème de Goldbach*, Videnskabsselskabet i Kristiania Skrifter I, Matematisk-Naturvidenskapelig Klasse No. 3 (1920) pp. 1-36.

[4] G. H. Hardy e J. E. Littlewood, *Some problems of 'partitio numerorum'; III: On the expression of a number as a sum of primes*, Acta Math. 44 (1923), 1–70.

[5] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. Math. 31 (1930), 419–448. Reimpresso em *Selected Papers*, (ed. D. McCarthy), vol 1, Ch. Babbage Res. Center, St. Pierre, Manitoba, Canada, 11–48 (1981).

[6] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. 1 (1878), 184–240 e 289–321.