6 Pseudoprimos

§ 6.1

O Pequeno Teorema de Fermat nos diz que, se n é primo, então temos $b^n \equiv b \pmod{n}$ para todo $b \in \mathbb{Z}$. Portanto, a contrapositiva diz que se temos

$$b^n \not\equiv b \pmod{n} \tag{$*$}$$

para *algum* $b \in \mathbb{Z}$, então n é composto!

Como todo $b \in \mathbb{Z}$ é congruente módulo n a algum *natural* menor do que n, então se existe algum $b \in \mathbb{Z}$ satisfazendo $(*)$, existe também algum b que satisfaz $(*)$ e $0 \le b < n$. Como para $b = 0$ ou $b = 1$ temos $b^n \equiv b \pmod{n}$, então se b satisfaz $(*)$, temos $1 < b < n$. E ainda mais, como estamos interessados apenas no caso n ímpar (por quê?), então

$$\begin{aligned}(n-1)^n &\equiv (-1)^n \\ &\equiv -1 \\ &\equiv n-1 \pmod{n},\end{aligned}$$

logo se b satisfaz $(*)$, temos $1 < b < n-1$. Resumindo:

Teorema 1 (Teste de primalidade de Fermat)**.** *Sejam n um inteiro positivo ímpar e b um inteiro tal que $1 < b < n-1$. Se $b^n \not\equiv b \pmod{n}$, então n é composto.*

Um b satisfazendo a hipótese do teste de Fermat é chamado testemunha (de Fermat) para n.

Exemplo 2. *Seja $R(229)$ o número $111\cdots1$, com 229 ocorrências do algarismo 1. Usando um computador, vemos que $2^{R(229)} \not\equiv 2 \pmod{R(229)}$; logo $R(229)$ é composto.*

Cuidado! O teste de Fermat permite concluir que n é composto se encontrarmos *alguma* testemunha, mas a recíproca não é *sempre* válida. Em outras palavras, **não** é sempre verdade que se n é um inteiro positivo e b satisfaz $1 < b < n-1$ e $b^n \equiv b \pmod{n}$, então n é primo:

Exemplo 3. *Para $n = 341$ e $b = 2$, temos $b^n \equiv b \pmod{n}$, mas $341 = 11 \cdot 31$ não é primo.*

Portanto, se no teste de Fermat para um dado b encontramos $b^n \equiv b \pmod{n}$, então o teste é inconclusivo.

Definição 4. Seja n e b inteiros positivos tais que n é composto e $1 < b < n-1$. Se $b^n \equiv b \pmod{n}$, então chamamos n de pseudoprimo para a base b.

Exemplo 5. *Como vimos, 341 é pseudoprimo para a base 2; entretanto, como $3^{341} \equiv 168 \pmod{341}$, podemos ver que 341* não *é pseudoprimo para a base 3.*

Entretanto, existem números que são compostos porém pseudoprimos para todas as bases!

§ 6.2

Definição 6. Um inteiro positivo ímpar n é um número de Carmichael se é pseudoprimo para toda base b.

Existem infinitos números de Carmichael, mas não provaremos isso neste curso.

Exemplo 7. *O menor número de Carmichael é 561. Isso pode ser verificado usando um computador e força bruta, mostrando que 561 é pseudoprimo para cada uma das bases* $b = 2, 3, 4, \ldots, 559$*. Feito isto, concluímos que* 561 *é um número de Carmichael. Claro que este método se torna completamente impraticável para números grandes; uma ideia melhor é a seguinte.*

Temos $561 = 3 \cdot 11 \cdot 17$*; na § 2.6 vimos o seguinte resultado.*

Lema (§ 2.6)**.** *Se a e b são coprimos, então ab divide c se, e somente se, ambos a e b dividem c.*

Na linguagem da aritmética modular, e já adaptando ao caso que nos interessa, podemos escrever este resultado assim:

Lema (§ 2.6, reescrito)**.** *Se a e b são coprimos, então $c \equiv d \pmod{ab}$ se, e somente se, $c \equiv d \pmod{a}$ e $c \equiv d \pmod{b}$.*

Logo, dado b com $1 < b < n-1$, para concluirmos $b^{561} \equiv b \pmod{561}$, basta concluirmos separadamente

$$\begin{aligned} b^{561} &\equiv b \pmod{3} \\ b^{561} &\equiv b \pmod{11} \\ b^{561} &\equiv b \pmod{17}. \end{aligned}$$

(Importante: note que aqui estamos usando o fato de que os fatores primos de 561 *têm multiplicidade* 1*, i.e., eles são todos distintos.)*

Agora basta calcular! Por exemplo, para o caso 11*, se b for múltiplo de* 11 *então de fato $b^{561} \equiv b \pmod{11}$ já que ambos os lados são* $0 \pmod{11}$*. Se b não for múltiplo de* 11*, então* $\mathrm{mdc}(b, 11) = 1$ *já que* 11 *é primo. Logo, pelo Pequeno Teorema de Fermat em sua segunda forma, temos* $b^{10} \equiv 1 \pmod{11}$*. Assim, como* 561 *dividido por* 10 *tem quociente* 56 *e resto* 1*, temos*

$$\begin{aligned} b^{561} &\equiv \left(b^{10}\right)^{56} \cdot b \\ &\equiv b \pmod{11}, \end{aligned}$$

como desejado. Com o mesmo raciocínio, concluímos $b^{561} \equiv b \pmod{11}$ e $b^{561} \equiv b \pmod{17}$, o que conclui a prova de que 561 *é um número de Carmichael.*

Recapitulando, no exemplo acima usamos alguns fatos cruciais sobre o número 561 na prova de que ele é um número de Carmichael:

1. Os fatores primos de 561 são distintos;
2. Cada fator primo p de 561 é tal que n dividido por $p-1$ deixa resto 1, i.e., $p-1$ divide $n-1$.

Na verdade, de certa forma a nossa prova usa *apenas* estes fatos; em outras palavras, ela se adapta para provar que qualquer n satisfazendo as condições (1) e (2) acima é um número de Carmichael:

Teorema (Teorema de Korselt, parte 1)**.** *Seja n um inteiro positivo ímpar. Se todo fator primo p de n satisfaz*

1. *p^2 não divide n (i.e., a multiplicidade de p como fator de n é 1);*
2. *$p-1$ divide $n-1$,*

então n é um número de Carmichael.

A adaptação da prova do caso $n = 561$ para o caso geral é um exercício.

Parece muita sorte encontrar n satisfazendo as propriedades do Teorema de Korselt acima. Supreendentemente, a recíproca do teorema é verdadeira e existem infinitos números de Carmichael!

Teorema (Teorema de Korselt, parte 2)**.** *Seja n um inteiro positivo ímpar. Se n é um número de Carmichael então todo fator primo p de n satisfaz*

1. *p^2 não divide n;*
2. *$p-1$ divide $n-1$,*

.

Prova parcial. Para mostrar que se n é um número de Carmichael então p^2 não divide n, mostraremos a contrapositiva: se p^2 divide n para algum fator primo p de n, então n não é um número de Carmichael, i.e., existe algum $b \in \mathbb{Z}$ tal que $b^n \not\equiv b \pmod{n}$. Na verdade, neste caso tomaremos $b = p$. Queremos então mostrar que $p^n \not\equiv p \pmod{n}$, i.e., que n não divide $p^n - p$. Como

$$p^n - p = p(p^{n-1} - 1)$$

e p não divide $p^{n-1}-1$ (já que p divide p^{n-1} e p não pode dividir dois números consecutivos), concluímos que p^2 não divide $p^n - p$. Mas estamos supondo que p^2 divide n; logo n não pode dividir $p^n - p$, i.e., $p^n \not\equiv p \pmod{n}$, como desejado.

Para mostrar que se n é um número de Carmichael então $p-1$ divide $n-1$ para qualquer fator primo p de n, vamos usar os seguintes resultados do futuro:

Lema (Lema Chave, § 9.1)**.** *Sejam* $a \in \mathbb{Z}$ *e* $n \in \mathbb{N}$*. Se* x *é o menor natural tal que* $\overline{a}^x = \overline{1}$ *em* $\mathbb{Z}_n$*, e* y *é* algum *natural tal que* $\overline{a}^y = \overline{1}$ *em* $\mathbb{Z}_n$*, então* x *divide* y*.*

Teorema (Teorema da Raiz Primitiva, § 10.1)**.** *Se* p *é primo, então existe* $a \in \mathbb{Z}$ *tal que*

1. $\mathrm{mdc}(a, p) = 1$ *e*

2. *o menor* x *para o qual temos* $\overline{a}^x = 1$ *em* $\mathbb{Z}_p$ *é* $x = p - 1$*.*

Então suponha que n seja um número de Carmichael e seja p um fator primo de n. Seja $a \in \mathbb{Z}$ como no Teorema da Raiz Primitiva. Como n é um número de Carmichael, temos $a^n \equiv a \pmod{n}$, i.e., n divide $a^n - a$. Como p divide n, concluímos que p também divide $a^n - a$, i.e.,

$$a^n \equiv a \pmod{p}. \qquad (**)$$

Mas $\mathrm{mdc}(a, p) = 1$, i.e., a é inversível módulo p. Multiplicando ambos os lados de $(**)$ pelo inverso de a módulo p, obtemos $a^{n-1} \equiv 1 \pmod{p}$, i.e.,

$$\overline{a}^{n-1} = \overline{1} \qquad \text{em } \mathbb{Z}_p. \qquad (***)$$

Finalmente, como pelo Teorema da Raiz Primitiva o menor x para o qual $\overline{a}^x = \overline{1}$ em $\mathbb{Z}_p$ é $x = p - 1$, usando o Lema Chave concluímos que $(***)$ implica que $p - 1$ divide $n - 1$, como queríamos. ■

§ 6.3 Teste de Miller (–Rabin)

Em $\mathbb{Z}$ (na verdade, nos números complexos), há exatamente duas soluções para a equação

$$x^2 = 1;$$

$x = \pm 1$. Quando passamos para $\mathbb{Z}_n$, isso pode deixar de ser verdade; por exemplo, em $\mathbb{Z}_8$ temos $\overline{3}^2 = \overline{1}$, mas $\overline{3} \neq \overline{1}$ e $\overline{3} \neq \overline{-1}$.

Lema. *Se* n *é primo, então em* $\mathbb{Z}_n$ *a equação*

$$x^2 = \overline{1}$$

só tem as soluções $x = \overline{1}$ *e* $x = \overline{-1}$*. Em outras palavras, se* n *é primo e*

$$a^2 \equiv 1 \pmod{n},$$

então

$$a \equiv 1 \pmod{n} \qquad \textit{ou} \qquad a \equiv -1 \pmod{n}.$$

Prova. Suponha que $x = \overline{a}$ seja solução de $x^2 = \overline{1}$ em $\mathbb{Z}_n$. Em outras palavras,

$$a^2 \equiv 1 \pmod{n},$$

ou seja,

$$\begin{aligned}(a+1)(a-1) &\equiv a^2 - 1 \\ &\equiv 0 \pmod{n},\end{aligned}$$

i.e., n divide $(a+1)(a-1)$. Como n é primo, isso implica que n divide $a+1$ ou divide $a-1$, i.e.,

$$a \equiv 1 \pmod{n} \qquad \text{ou} \qquad a \equiv -1 \pmod{n};$$

em outras palavras, em $\mathbb{Z}_n$,

$$\overline{a} = \overline{1} \qquad \text{ou} \qquad \overline{a} = \overline{-1}. \qquad \blacksquare$$

Esse é o lema central que usaremos no teste de Miller–Rabin; pela contrapositiva, se $x^2 = \overline{1}$ tem alguma solução diferente de $x = \pm\overline{1}$ em $\mathbb{Z}_n$, então n é composto.

A ideia é a seguinte: <u>se n é primo</u>, então pelo PTF(2) para qualquer b com $1 < b < n-1$ temos

$$b^{n-1} \equiv 1 \pmod{n}.$$

Como estamos interessados no caso em que n é ímpar, então existe algum k_0 inteiro tal que $n - 1 = 2k_0$. Mas então $b^{n-1} = (b^{k_0})^2$, e pelo Lema § 6.3 temos

$$b^{k_0} \equiv 1 \pmod{n} \qquad \text{ou} \qquad b^{k_0} \equiv -1 \pmod{n}.$$

<u>Se</u> $b^{k_0} \equiv 1 \pmod{n}$ <u>e</u> k_0 é par, digamos $k_0 = 2k_1$, então novamente pelo Lema § 6.3 temos

$$b^{k_1} \equiv 1 \pmod{n} \qquad \text{ou} \qquad b^{k_1} \equiv -1 \pmod{n}.$$

Novamente, <u>se</u> $b^{k_1} \equiv 1 \pmod{n}$ <u>e</u> k_1 é par, digamos $k_1 = 2k_2$, então pelo Lema § 6.3 temos

$$b^{k_2} \equiv 1 \pmod{n} \qquad \text{ou} \qquad b^{k_2} \equiv -1 \pmod{n},$$

e assim por diante, até que encontremos um k_m tal que $b^{k_m} \equiv -1$ <u>ou</u> $b^{k_m} \equiv 1$ com k_m ímpar.

Portanto, se esse processo "falha" em algum momento, então n tem que ser um número composto. Mais precisamente, trabalhamos em ordem reversa. Tomemos b com $1 < b < n-1$. Primeiro, fazendo sucessivas divisões por 2 decompomos o número par $n-1$ na forma $n-1 = 2^k q$, com q ímpar. Agora, se

$$b^q \equiv \pm 1 \pmod{n}$$

demos azar e nada podemos concluir. Senão, pelo Lema, se

$$b^{2q} \equiv 1 \pmod{n},$$

então n é composto, mas se

$$b^{2q} \equiv -1 \pmod{n},$$

demos azar e nada podemos concluir. Por outro lado, se

$$b^{2q} \not\equiv \pm 1 \pmod{n},$$

então novamente pelo Lema, se

$$b^{4q} \equiv 1 \pmod{n},$$

então n é composto, mas se

$$b^{4q} \equiv -1 \pmod{n},$$

demos azar e nada podemos concluir, e assim sucessivamente.

Algoritmo 2: Teste de Miller–Rabin

Entrada: Um inteiro positivo primo n e um inteiro b com $1 < b < n-1$

Saída: Uma das mensagens "n é composto" ou "teste inconclusivo"

Passo 1: Encontre k tal que $n-1 = 2^k q$ com q ímpar, e faça

$$i \leftarrow 0$$
$$r \leftarrow \text{resto da divisão de } b^q \text{ por } n$$

Passo 2: Se $r = n-1$, então retorne "teste inconclusivo".
Senão, se $r = 1$:

- se $i = 0$, então retorne "teste inconclusivo"
- se $i > 0$, então retorne "n é composto".

Senão, se $i = k$, retorne "n é composto".
Senão, vá para o Passo 3.

Passo 3: Faça

$$i \leftarrow i + 1$$
$$r \leftarrow \text{resto da divisão de } r^2 \text{ por } n$$

e vá para o Passo 2.

Os enunciados e provas dos Teoremas de Finitude e Corretude do teste de Miller–Rabin fazem parte da lista de exercícios para este capítulo.

Exemplo 8. *Vamos considerar o caso* $n = 341$ *com a base* $b = 2$*, lembrando que* 341 *é pseudoprimo para esta base (i.e., o teste de Fermat com base* $b = 2$ *não detecta que* b *é composto). Temos* $341 - 1 = 340 = 2^2 \cdot 85$*. Agora podemos fazer uma tabela mostrando a execução do Teste de Miller–Rabin:*

i	r	
0	32	*pois* $2^{85} \equiv 32 \pmod{341}$
1	1	*pois* $2^{2\cdot 85} \equiv 32^2 \equiv 1 \pmod{341}$

Logo o teste de Miller–Rabin detecta que 341 *é composto.*

Agora consideremos o caso $n = 561$*, que é um número de Carmichael (i.e., é pseudoprimo para todas as bases, ou seja, não é detectado como composto pelo teste de Fermat com nenhuma base), novamente com a base* $b = 2$*. Temos* $560 = 2^4 \cdot 35$*. Tabelando a execução do Teste de Miller–Rabin:*

i	r	
0	263	*pois* $2^{35} \equiv 263 \pmod{561}$
1	166	*pois* $2^{2\cdot 35} \equiv 263^2 \equiv 166 \pmod{561}$
2	67	*pois* $2^{2^2\cdot 35} \equiv 166^2 \equiv 67 \pmod{561}$
3	1	*pois* $2^{2^3\cdot 35} \equiv 67^2 \equiv 1 \pmod{561}$

Logo, novamente o teste de Miller–Rabin detecta que 561 é composto.

Consideremos agora $n = 2047$ *e* $b = 2$*. Temos* $2047 - 1 = 2046 = 2 \cdot 1023$*, e:*

i	r	
0	1	*pois* $2^{1023} \equiv 1 \pmod{2047}$,

logo o teste de Miller–Rabin é inconclusivo para $n = 2047$ *e* $b = 2$*. Por outro lado, com* $b = 3$ *temos*

i	r	
0	1565	*pois* $3^{1023} \equiv 1565 \pmod{2047}$
1	1013	*pois* $3^{2\cdot 1023} \equiv 1565^2 \equiv 1013 \pmod{2047}$,

portanto o teste de Miller–Rabin detecta que $n = 2047$ *é composto com a base* $b = 3$.

Definição 1. Sejam n número inteiro positivo composto ímpar e b um inteiro tal que $1 < b < n - 1$. Se o teste de Miller–Rabin com n e b com entradas detecta que n é composto, então chamamos b de uma testemunha de Miller–Rabin para n. Caso contrário, se o teste de Miller–Rabin com entradas n e b é inconclusivo, dizemos que n é um pseudoprimo forte para a base b, ou pseudoprimo de Miller–Rabin para a base b. Em outras palavras, n é pseudoprimo forte para a base b se, tomando k tal que $n - 1 = 2^k \cdot q$ para algum q ímpar, temos

1. $b^q \equiv 1 \pmod{n}$; ou

2. $b^{2^i \cdot q} \equiv -1 \pmod{n}$ para algum natural $i < k$.

Como veremos na lista de exercícios deste capítulo, qualquer número que seja pseudoprimo forte para uma certa base também é pseudoprimo (de Fermat) para aquela base, mas também já vimos nos exemplos que a recíproca não é verdadeira (por exemplo, para $n = 341$ e $b = 2$). Na verdade, por exemplo, só existem 1282 pseudoprimos fortes para a base 2 dentre os números compostos até 10^9. Portanto, o teste de Miller–Rabin já seria mais vantajoso que o de Fermat apenas por este motivo.

Mas sabemos bem mais:

Teorema (Rabin)**.** *Um inteiro positivo composto ímpar n tem pelo menos $\frac{3n}{4}$ testemunhas de Miller–Rabin dentre as bases b com $1 < b < n - 1$.*

A prova deste teorema está além do nosso alcance nesta disciplina, mas a sua utilidade é clara: se quisermos saber se n é primo e tomamos uma base b *aleatoriamente* no intervalo $1 < b < n - 1$, caso a resposta do teste seja inconclusiva, nossa confiança de que n é de fato primo é de aproximadamente $3/4 = 75\%$! Se fizermos outro teste com base b' diferente mas também sorteada aleatoriamente neste intervalo, um teste inconclusivo eleva nossa certeza sobre a primalidade de n para aproximadamente $15/16 = 93,75\%$; com mais um teste inconclusivo, a certeza vai a $63/64 = 98,4375\%$, e assim por diante. Desta forma, com apenas uma quantidade pequena de testes, nossa certeza sobre a primalidade de n pode ser tornada maior do que a certeza, por exemplo, de que não houve alguma falha no hardware do computador ao efetuar as contas em algum teste completamente determinístico.

Finalmente, apenas por curiosidade:

Teorema (Miller)**.** *Se a* Conjectura Generalizada de Riemann *é verdadeira, então qualquer inteiro positivo composto ímpar n tem alguma testemunha de Miller–Rabin menor do que* $2 \cdot (\ln n)^2$.