NÚMEROS INTEIROS E CRIPTOGRAFIA – UFRJ

GABARITO LISTA 3: FATORAÇÃO E PRIMOS

1. Ver gabarito das questões do livro.

2. Suponhamos que n tenha como fatoração
$$n = p_1^{e_1} \cdots p_s^{e_s}$$
em que $1 < p_1 < \cdots < p_s$ são fatores primos e os expoentes $e_1, \ldots, e_s$ são todos positivos. Como p_1 é o maior fator primo de n, temos da hipótese da questão que
$$n^{1/3} < p_1 < \cdots < p_s.$$
Substituindo estas desigualdades na fatoração de n,
$$n = p_1^{e_1} \cdots p_s^{e_s} > (n^{1/3})^{e_1} \cdots (n^{1/3})^{e_s} = n^{(e_1+\cdots+e_s)/3}.$$
Mas, para que isto seja verdade, devemos ter que
$$\frac{(e_1 + \cdots + e_s)}{3} < 1;$$
que equivale a dizer que
$$(e_1 + \cdots + e_s) < 3,$$
que só pode ocorrer se a fatoração de n for de uma das seguintes formas
$$p_1, \quad p_1^2 \quad \text{ou} \quad p_1 p_2.$$
Logo, n não pode ter mais de um fator primo, como afirmado na questão.

3. Como $\sqrt{6883901} = 2623.7189$ não é inteiro, construímos a tabela começando da parte inteira da raiz quadrada mais um, isto é, de 2624.

x	$\sqrt{x^2 - n}$	inteiro?
2624	38.40	não
2625	82	sim

Portanto, os fatores desejados são
$$x - y = 2625 - 82 = 2543 \quad \text{e} \quad x + y = 2625 + 82 = 2707.$$

4. Como $\sqrt{6883901} = 2623.7189$ não é inteiro, construímos a tabela começando da parte inteira da raiz quadrada mais um, isto é, de 2624.

x	$\sqrt{x^2-n}$	inteiro?
1000,0	25,16	não
1001,0	51,323	não
1002,0	68,096	não
1003,0	81,499	não
1004	93	sim

Portanto, os fatores desejados são

$$x - y = 1004 - 93 = 911 \quad \text{e} \quad x + y = 1004 + 93 = 1097.$$

5. (a) Comparando $n = x^2 - y^2$ com $n = pq$, temos que

$$(x-y)(x+y) = pq,$$

donde $x - y = p$ e $x + y = q$, já que $p < q$. Resolvendo os dois sistemas lineares, obtemos

$$x = \frac{q+p}{2} \text{ e } y = \frac{q-p}{2}.$$

(b) Como o algoritmo inicia o cálculo da tabela a partir de $[\sqrt{n}]+1$, então o número de x que precisa tentar até fatorar n é igual a

$$[\sqrt{n}] + 1 - \frac{q+p}{2}.$$

6. (a) Em primeiro lugar, cada p_i divide N, então S é inteiro. Por outro lado, se $i \neq j$ então p_i divide N/p_j. Portanto, se supusermos, por contradição, que p_i divide S, então p_i também divide

$$S - \left(\frac{N}{p_1} + \frac{N}{p_2} + \frac{N}{p_{i-1}} + \cdots + \frac{N}{p_{i+1}} + \cdots + \frac{N}{p_r}\right) = \frac{N}{p_i}.$$

Mas N/p_i é um produto de primos diferentes de p_i, de modo que obtivemos uma contradição pelo teorema da fatoração única. Portanto, p_i não pode dividir S.

(b) Suponhamos, por contradição, que haja apenas uma quantidade finita de primos, digamos $p_1 < \cdots < p_r$. Tome $N = p_1 p_2 \cdots p_r$ e seja

$$S = \frac{N}{p_1} + \cdots + \frac{N}{p_r}.$$

Então S tem que ter um fator primo pelo teorema da fatoração única. Mas por (1) este fator tem que ser diferente de todos os primos $p_1, \ldots, p_r$. Como

estamos supondo que estes são todos os primos que existem, temos uma contradição.

Esta demonstração da infinidade dos primos foi dada originalmente por Métrod em 1917.

7. (a) Suponha que haja um número finito de primos, todos menores que $n \geq 3$. Então $n! \geq 2$ e $n! - 1 \geq 3$. Portanto, ambos são inteiros maiores ou iguais a 2, e pelo Teorema da Fatoração Única ambos têm fatores primos. Entretanto, como todos os primos são menores que n, então todos são fatores de $n!$. Portanto, qualquer que seja o fator primo de $n! - 1$, ele terá que dividir $n!$. Em particular, $n!$ e $n! - 1$ têm um fator comum, de modo que seu máximo divisor comum não pode ser igual a 1.

(b) Como $\text{mdc}(n!, n! - 1)$ divide $n!$ e $n! - 1$, então deve dividir $n! - (n! - 1) = 1$. Mas isto implica que $\text{mdc}(n!, n! - 1) = 1$, contradizendo (1). isto significa que a hipótese feita, no início da questão, de que todos os primos são menores que n tem que estar errada. Portanto, não existe nenhum inteiro $n \geq 3$ que seja maior que todos os primos. Mas isto só pode acontecer se houver infinitos números primos.

Se você encontrar algum erro no gabarito, por favor comunique ao professor através do endereço `collier@dcc.ufrj.br`. Qualquer dúvida entre em contato com os monitores via Facebook. As aulas de monitoria serão nas segundas-feiras 13h-15h