Teorija števil

1. Zgornji in spodnji celi del
2. Deljivost in Evklidov algoritem
3. Linearna diofantska enačba z dvema neznankama
4. Praštevila
5. Kongruenca
6. Eulerjeva funkcija
7. Uporaba v kriptografiji

Zgornji in spodnji celi del

Spodnji celi del

$$\lfloor x \rfloor = \max\{k \in \mathbb{Z};\, k \leq x\}$$

Zgornji celi del

$$\lceil x \rceil = \min\{k \in \mathbb{Z};\, k \geq x\}$$

Zgledi:

Lastnosti:

1. $x \in \mathbb{Z} \;\Leftrightarrow\; x = \lfloor x \rfloor \;\Leftrightarrow\; x = \lceil x \rceil$
2. $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \quad \text{in} \quad x - 1 < \lfloor x \rfloor \leq x$
3. $\lceil x \rceil - 1 < x \leq \lceil x \rceil \quad \text{in} \quad x \leq \lceil x \rceil < x + 1$
4. Za poljuben $k \in \mathbb{Z}$ imamo
$$\begin{aligned} \lfloor x + k \rfloor &= \lfloor x \rfloor + k \\ \lceil x + k \rceil &= \lceil x \rceil + k \end{aligned}$$
5. $\lceil x \rceil = -\lfloor -x \rfloor \quad \text{in} \quad \lfloor x \rfloor = -\lceil -x \rceil$
6. $\lceil x \rceil = \begin{cases} \lfloor x \rfloor & x \in \mathbb{Z} \\ \lfloor x \rfloor + 1 & \text{sicer} \end{cases} \quad \text{ter} \quad \lfloor x \rfloor = \begin{cases} \lceil x \rceil & x \in \mathbb{Z} \\ \lceil x \rceil - 1 & \text{sicer.} \end{cases}$

Problem 1 *Za $m, n \in \mathbb{N}$ izračunaj, koliko je naravnih števil med 1 in n deljivih z m.*

Rešitev: To so števila $m, 2m, 3m, \ldots, k\,m$, kjer je $k\,m \leq n$ in $(k+1)\,m > n$. Tako je k iskano število. Velja

$$k \leq \frac{n}{m} \quad \text{in} \quad k+1 > \frac{n}{m},$$

od tod pa dobimo, da je $k = \lfloor \frac{n}{m} \rfloor$.

Problem 2 *Za $n \in \mathbb{N}$ in p praštevilo poišči eksponent praštevila p v razcepu števila $n!$ na prafaktorje.*

Rešitev: Ker je $n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$ iz prejšnje naloge sledi, da je število faktorjev deljivih s p $\lfloor \frac{n}{p} \rfloor$. Število faktorjev deljivih s p^2 je $\lfloor \frac{n}{p^2} \rfloor$. Število faktorjev deljivih s p^3 je $\lfloor \frac{n}{p^3} \rfloor$, itd.

Tako sklepamo, da je iskano število enako vsoti:

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^k} \right\rfloor,$$

kjer je $k \in \mathbb{N}$ število, za katerega velja $p^k \leq n < p^{k+1}$ tj. $k = \lfloor \lg_p n \rfloor$.

Naloga 1 *Poišči eksponent praštevila 5 v razcepu števila 2007! na prafaktorje.*

Deljivost celih števil

Za števila $m, n \in \mathbb{Z}$ pravimo, da m **deli** n ter pišemo $m \mid n$, če obstaja število $k \in \mathbb{Z}$ tako, da je $n = k \cdot m$.

Rečemo tudi:

- n **je deljiv z** m
- m **je delitelj** n
- n **je večkratnik** m

Če m ni delitelj n, potem pišemo $m \nmid n$.

Zgledi:

- $3 \mid 2007$, ker je $2007 = 669 \cdot 3$;
- $5 \nmid 2007$, ker je $401 \cdot 5 < 2007 < 402 \cdot 5$.

Naj bo n celo število. Potem velja:

- $1 \mid n$, ker je $n = n \cdot 1$;
- $n \mid n$, ker je $n = 1 \cdot n$;
- $n \mid 0$, ker je $0 = n \cdot 0$;
- $n \mid -n$, ker je $-n = (-1) \cdot n$.

Lastnosti relacije $\mid$

1. *refleksivnost*: $n \mid n$

2. *tranzitivnost*:
$$\begin{aligned} k \mid m \wedge m \mid n &\Rightarrow \exists p \in \mathbb{Z} : m = p \cdot k \wedge \exists q \in \mathbb{Z} : n = q \cdot m \\ &\Rightarrow \exists p, q \in \mathbb{Z} : n = (p \cdot q) \cdot k \\ &\Rightarrow \exists r \in \mathbb{Z} : n = r \cdot k \\ &\Rightarrow k \mid n \end{aligned}$$

3. *antisimetričnost na* $\mathbb{N}$:
$$\begin{aligned} n \mid m \wedge m \mid n &\Rightarrow \exists p \in \mathbb{N} : m = n \cdot p \wedge \exists q \in \mathbb{N} : n = m \cdot q \\ &\Rightarrow \exists p, q \in \mathbb{N} : n = (p \cdot q) \cdot m \\ &\Rightarrow p = q = 1 \\ &\Rightarrow m = n \end{aligned}$$

4. *delna urejenost na* $\mathbb{N}$: sledi iz lastnosti 1.-3.

5. *Če* $m \mid a$ *in* $m \mid b$, *potem* $m \mid a + b$:
$$\begin{aligned} m \mid a \wedge m \mid b &\Rightarrow \exists p \in \mathbb{Z} : a = p \cdot m \wedge \exists q \in \mathbb{Z} : b = q \cdot m \\ &\Rightarrow \exists p, q \in \mathbb{Z} : a + b = (p + q) \cdot m \\ &\Rightarrow \exists r \in \mathbb{Z} : a + b = r \cdot m \\ &\Rightarrow m \mid a + b \end{aligned}$$

6. *Če* $m \mid a$, *potem za vsak* $n \in \mathbb{Z}$ *velja* $m \mid n \cdot a$:
$$\begin{aligned} m \mid a \wedge n \in \mathbb{Z} &\Rightarrow \exists p \in \mathbb{Z} : a = p \cdot m \\ &\Rightarrow \exists p \in \mathbb{Z} : n \cdot a = (p \cdot n) \cdot m \\ &\Rightarrow \exists r \in \mathbb{Z} : n \cdot a = r \cdot m \\ &\Rightarrow m \mid n \cdot a \end{aligned}$$

Izrek o deljenju (ID)

Izrek 1 *Naj bosta $n, m \in \mathbb{Z}$ ter $m > 0$. Potem obstajata enoličnо določena $k, r \in \mathbb{Z}$ tako, da je*

$$n = k \cdot m + r \quad in \quad 0 \leq r < m. \tag{1}$$

Rečemo ter pišemo:

- k je **kvocient** oz. **količnik** števil n in m;
- r je **ostanek** pri deljenju števila n z m.
- $r = n \bmod m$.

Dokaz. Naj bo $k = \lfloor \frac{n}{m} \rfloor$ in $r = n - k \cdot m$. Potem:

$$\begin{array}{rcccl}
\frac{n}{m} - 1 & < & \lfloor \frac{n}{m} \rfloor & \leq & \frac{n}{m} \\
\frac{n}{m} - 1 & < & k & \leq & \frac{n}{m} \\
n - m & < & k \cdot m & \leq & n \\
m - n & > & -k \cdot m & \geq & -n \\
m & > & n - k \cdot m & \geq 0 & \\
m & > & r & \geq 0. &
\end{array}$$

Pokažimo še enoličnost. Recimo, da (1) velja tudi za par k_1, r_1. Tako imamo

$$n = k \cdot m + r = k_1 \cdot m + r_1.$$

Od tod $(k - k_1) \cdot m = r_1 - r$. Torej $m \mid r_1 - r$. Ker je $-m < r_1 - r < m$, sledi da je $r_1 - r = 0$, tj. $r_1 = r$. Iz tega pa tudi sledi, da je $k_1 = k$. $\square$

Zgledi:

- $17 \bmod 3 = 2$, ker je $17 = 5 \cdot 3 + 2$ in $0 \leq 2 < 3$;
- $(-17) \bmod 3 = 1$, ker je $-17 = (-6) \cdot 3 + 1$ in $0 \leq 1 < 3$.

Največji skupni delitelj. Če $m, n \in \mathbb{Z}$ nista 0, potem ga definiramo takole:

$$\gcd(m, n) = \max\{d \in \mathbb{N};\ d \mid m \text{ in } d \mid n\},$$

sicer $\gcd(0, n) = n$.

Najmanjši skupni večkratnik. Če $m, n \in \mathbb{Z}$ nista oba 0, potem ga definiramo takole:

$$\operatorname{lcm}(m, n) = \min\{v \in \mathbb{N};\ m \mid v \text{ in } n \mid v \text{ in } v > 0\},$$

sicer $\operatorname{lcm}(0, n) = 0$.

Zgled: $\gcd(20, 30) =$ $\operatorname{lcm}(20, 30) =$

$\gcd(0, 5) =$ $\operatorname{lcm}(0, 5) =$

Trditev 2 *Naj bo n skupni večkratnik števil a in b. Potem* $\operatorname{lcm}(a, b) \mid n$.

Dokaz. Po izreku o deljenju naj bo $n = k \cdot \operatorname{lcm}(a, b) + r$ in $0 \leq r < \operatorname{lcm}(a, b)$. Potem je $r = k \cdot \operatorname{lcm}(a, b) - n$ skupni večkratnik števil a in b. Zato iz $0 \leq r < \operatorname{lcm}(a, b)$ sledi, da je $r = 0$.

Evklidov algoritem

Trditev 3 *Naj bo* $a = k\,b + r$ *ter* $0 \leq r < b$. *Potem*

$$\gcd(a, b) = \gcd(b, r).$$

Dokaz. Velja naslednje

$$\begin{aligned} m \mid a \text{ in } m \mid b &\Rightarrow m \mid a - k\,b \Rightarrow m \mid r \\ m \mid b \text{ in } m \mid r &\Rightarrow m \mid k\,b + r \Rightarrow m \mid a \end{aligned}$$

Zgornja izpeljava nam zagotovi, da je poljubno število m delitelj števil a in b natanko takrat, ko je delitelj števil b in r, tj.

$$\begin{aligned} \{m \in \mathbb{N};\, m \mid a \text{ in } m \mid b\} &= \{m \in \mathbb{N};\, m \mid b \text{ in } m \mid r\} \\ \max\{m \in \mathbb{N};\, m \mid a \text{ in } m \mid b\} &= \max\{m \in \mathbb{N};\, m \mid b \text{ in } m \mid r\} \\ \gcd(a, b) &= \gcd(b, r). \end{aligned}$$

□

Zgled: Izračunajmo $\gcd(899, 812)$!

Velja

$$\begin{aligned} 899 &= 1 \cdot 812 + 87 \\ 812 &= 9 \cdot 87 + 29 \\ 87 &= 3 \cdot 29 + 0. \end{aligned}$$

Torej

$$\gcd(899, 812) = \gcd(812, 87) = \gcd(87, 29) = \gcd(29, 0) = 29.$$

Razširjeni Evklidov algoritem (REA)

REA poišče ne le $\gcd(a, b)$, ampak tudi $s, t \in \mathbb{Z}$ tako, da velja

$$a \cdot s + b \cdot t = \gcd(a, b)\,.$$

Zgled: $a = 899$, $b = 812$, $\gcd(a, b) = 29$!

Velja

$$\begin{aligned} 29 &= 1 \cdot 812 - 9 \cdot 87 \\ &= 812 - 9 \cdot (899 - 1 \cdot 812) \\ &= 812 \cdot 10 + 899 \cdot (-9) \end{aligned}$$

Torej, $s = 10$ in $t = -9$.

REA postopek

- Začetne vrednosti:

$$\begin{array}{lll} r_{-1} = a & s_{-1} = 1 & t_{-1} = 0 \\ r_0 = b & s_0 = 0 & t_0 = 1 \end{array}$$

- Iteracija: za $i = 1, 2, \ldots, n+1$ izračunaj

$$\begin{aligned} k_i &= \lfloor \tfrac{r_{i-2}}{r_{i-1}} \rfloor \\ r_i &= r_{i-2} - k_i \cdot r_{i-1} \\ s_i &= s_{i-2} - k_i \cdot s_{i-1} \\ t_i &= t_{i-2} - k_i \cdot t_{i-1}, \end{aligned}$$

  kjer je $n+1$ najmanjši indeks, za katerega je $r_{n+1} = 0$.

Velja. $r_n = \gcd(a, b)$.

Prikaz postopka s tabelo:

	a	1	0
k_1	b	0	1
k_2	r_1	s_1	t_1
k_3	r_2	s_2	t_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
k_{n+1}	$r_n \neq 0$	s_n	t_n
	$r_{n+1} = 0$	s_{n+1}	t_{n+1}

Trditev 4 *Velja:*

- $a \cdot s_i + b \cdot t_i = r_i \ za \ i = -1, 0, \ldots n+1;$
- $r_n | r_i \ za \ i = n, n-1, \ldots, 0, -1;$
- $\gcd(a, b) = r_n.$

Dokaz. Prvo trditev pokažimo z indukcijo po i:

$$\begin{aligned}
i = -1: \quad a \cdot 1 + b \cdot 0 &= a \\
i = 0: \quad a \cdot 0 + b \cdot 1 &= b \\
i > 0: \quad a \cdot s_i + b \cdot t_i &= a\,(s_{i-2} - k_i s_{i-1}) + b\,(t_{i-2} - k_i \cdot t_{i-1}) \\
&= (a\,s_{i-2} + b\,t_{i-2}) - k_i\,(a\,s_{i-1} + b\,t_{i-1}) \\
&= r_{i-2} - k_i\,r_{i-1} \\
&= r_i\,.
\end{aligned}$$

Drugo trditev pokažemo z indukcijo po i nazaj:

$$\begin{aligned}
i = n: \quad & r_n \mid r_n \\
i = n-1: \quad & 0 = r_{n+1} = r_{n-1} - k_{n+1} \cdot r_n \text{ od tod } r_{n-1} = k_{n+1} \cdot r_n\,. \\
& \text{Torej } r_n \mid r_{n-1} \\
i \leq n-2: \quad & r_{i+2} = r_i - k_{i+2} \cdot r_{i+1} \text{ oziroma } r_i = k_{i+2} \cdot r_{i+1} + r_{i+2}. \\
& \text{Ker } r_n \mid r_{i+1} \text{ in } r_n \mid r_{i+2}, \text{ dobimo } r_n \mid r_i.
\end{aligned}$$

Pokažimo zadnjo trditev. Po drugi trditvi, $r_n \mid r_{-1} = a$ in $r_n \mid r_0 = b$, kar sledi, da je r_n skupni delitelj a in b. Če je d skupni delitelj a, b potem $d \mid a$ in $d \mid b$ in od tod $d \mid a \cdot s_n + b \cdot t_n = r_n$. Torej, $r_n = \gcd(a, b)$. $\square$

Prikaz postopka s tabelo:

	899	1	0
1	812	0	1
9	87	1	−1
3	29	−9	10
	0	28	−31

Tuji števili

Če je $\gcd(a,b) = 1$ za števili $a, b \in \mathbb{N}$, potem rečemo, da sta **tuji** ter pišemo $a \perp b$.

Zgled: $3 \perp 8,\ 12 \perp 35,\ 6 \not\perp 15\,.$

Trditev 5 *Za števila* $a, b, c \in \mathbb{N}$ *velja*

$$a \mid b\,c \quad \wedge \quad a \perp b \quad \Rightarrow \quad a \mid c.$$

Dokaz. Ker $a \mid b\,c$, obstaja $k \in \mathbb{Z}$ tako, da je $b\,c = k\,a$. Po (REA) iz $\gcd(a,b) = 1$ sledi

$$\exists s, t \in \mathbb{Z} : a\,s + b\,t = 1.$$

Zmnožimo s c zadnjo enačbo:

$$a\,s\,c + b\,t\,c = c,$$

zdaj vstavimo $b\,c = k\,a$ ter izpostavimo a

$$a\,(s\,c + t\,k) = c$$

in od tod sklepamo, da $a \mid c$. □

Trditev 6 *Za števili* $a, m \in \mathbb{N}$ *velja*

$$m \perp a \quad \Leftrightarrow \quad m \perp (a \bmod m).$$

Dokaz. Po (ID) naj bo $a = k\,m + r$ tj. $r = a \bmod m$. Potem iz (EA) sledi, da je $\gcd(a,r) = \gcd(a,m) = 1$. Torej je $m \perp r$ natanko takrat, ko je $m \perp (a \bmod m)$. □

Zveza med gcd **in** lcm

Izrek 7 *Za poljubni naravni števili a in b velja*

$$\gcd(a,b)\cdot \mathrm{lcm}(a,b) = a\cdot b\,.$$

Dokaz. Naj bo $d = \gcd(a,b)$ ter $a = a_1\,d$ in $b = b_1\,d$ za neka $a_1, b_1 \in \mathbb{N}$. Potem velja $a_1 \perp b_1$. Iz zveze

$$\frac{a\,b}{d} = a_1\,b_1\,d = a_1\,b = b_1\,a$$

sledi, da je $\frac{a\,b}{d}$ skupni večkratnik števil a in b.

Zdaj naj bo $v = \mathrm{lcm}(a,b)$ ter $v = a\,p$ in $v = b\,q$ za neka $p, q \in \mathbb{N}$. Potem

$$v \;=\; p\,a_1\,d \;=\; q\,b_1\,d \quad\Rightarrow\quad p\,a_1 \;=\; q\,b_1 \quad\Rightarrow\quad b_1 \mid p\,a_1.$$

Iz $a_1 \perp b_1$ sledi, da $b_1 \mid p$, tj. $p = k\,b_1$ za nek $k \in \mathbb{N}$. Torej

$$v \;=\; k\,a\,b_1 \;=\; k\,a_1\,b_1\,d \;\Rightarrow\; a_1\,b_1\,d \mid v$$

Ker pa je $a_1\,b_1\,d$ večkratnik od a in b, sklepamo, da je $v = a_1\,b_1\,d$, tj. $\frac{a\,b}{d} = v$. To pa je iskana zveza. □

Zgled: Preveri zgornji izrek za $a = 12$ ter $b = 15$.

Praštevila

Naravno število $n \geq 2$ je **praštevilo**, če ima natanko dva delitelja, 1 in n. Sicer je n **sestavljeno število**.

Zgled: Praštevila do 100 so 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Par praštevil oblike $(p, p+2)$ imenujemo **praštevilska dvojčka**.

Naloga 2 *Koliko je parov praštevilskih dvojčkov med* 1 *in* 100*?*

Trditev 8 *Naj bosta* a, b *naravni števili. Potem velja:*

1. *Če je* p *praštevilo, potem* $p \perp a$ *ali* $p \mid a$*;*
2. *Če je* p *praštevilo ter* $p \mid a \cdot b$*, potem* $p \mid a$ *ali* $p \mid b$*;*
3. *Za* $a \geq 2$ *obstaja praštevilo* p *tako, da* $p \mid a$*.*

Dokaz.

Izrek 9 (Evklid) *Praštevil je neskončno.*

Dokaz. Predpostavimo obratno, naj bodo $p_1, p_2, p_3 \ldots, p_{k-1}, p_k$ vsa praštevila. Obravnavajmo število

$$P = p_1\, p_2\, p_3 \cdots p_{k-1}\, p_k + 1$$

Velja $P \geq 2$ ter $P \bmod p_i = 1$ za $i = 1, 2, \ldots, k$. To pa je v protislovju s prejšnjo trditvijo.

Hipoteza 1 (Goldenberg) *Praštevilskih dvojčkov je neskončno mnogo.*

Kongruenca po modulu m

Naj bosta $a, b \in \mathbb{Z}$ ter $m \in \mathbb{N}$. Če $m \mid a - b$ potem rečemo, da sta a in b **kongruentna po modulu** m ter pišemo $a \equiv b \pmod{m}$.

Zgledi:

- $17 \equiv 26 \pmod{3}$
- $25 \not\equiv 18 \pmod{3}$
- $a \equiv b \pmod{2} \quad \Leftrightarrow \quad a$ in b sta enake parnosti.

Velja

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad a \bmod m = b \bmod m\,,$$

od tod pa sledi, da je $\equiv \pmod{n}$ ekvivalenčna relacija na $\mathbb{Z}$ ter je število razredov m – za vsak ostanek en razred.

Zgled:

Lastnosti kongruence:

1. Če $a \equiv b \pmod{m}$ ter $c \in \mathbb{Z}$, potem

$$\begin{aligned} a + c &\equiv b + c \pmod{m} \\ a - c &\equiv b - c \pmod{m} \\ a \cdot c &\equiv b \cdot c \pmod{m} \end{aligned}$$

2. Če $a \equiv b \pmod{m}$ ter $c \equiv d \pmod{m}$, potem

$$\begin{aligned} a + c &\equiv b + d \pmod{m} \\ a - c &\equiv b - d \pmod{m} \\ a \cdot c &\equiv b \cdot d \pmod{m} \end{aligned}$$

3. Če $a \equiv b \pmod{m}$ ter $n \in \mathbb{N}$, potem $a^n \equiv b^n \pmod{m}$.
4. Če $a \cdot c \equiv b \cdot c \pmod{m}$ ter $c \perp m$, potem $a \equiv b \pmod{m}$.

Naloga 3 *Izračunaj* $3^{2007} \bmod 13$.

Naloga 4 *Naj bosta* p *in* q *različni praštevili tako, da* $a \equiv b \pmod{p}$ *in* $a \equiv b \pmod{q}$. *Pokaži, da* $a \equiv b \pmod{p\,q}$.

Eulerjeva funkcija $\varphi(n)$

Za $n \in \mathbb{N}$ je **Eulerjeva funkcija** $\varphi(n)$ število naravnih števil med 1 in n, ki so tuja n, tj.

$$\varphi(n) = |\{k \in \mathbb{N};\, 1 \leq k \leq n \,\wedge\, k \perp n\}|.$$

Zgledi:

$$\begin{aligned} \varphi(4) &= 2 \qquad & 1, 2, 3, 4 \\ \varphi(5) &= 4 \qquad & 1, 2, 3, 4, 5 \\ \varphi(8) &= 4 \qquad & 1, 2, 3, 4, 5, 6, 7, 8 \end{aligned}$$

Trditev 10 *Za vsako praštevilo p velja $\varphi(p) = p - 1$.*

Dokaz. Trditev velja, ker je vsako izmed števil $1, 2, \ldots, p-1$ tuje s p.

Trditev 11 *Za praštevilo p velja $\varphi(p^n) = p^n - p^{n-1}$.*

Dokaz. Če poljubno število ni tuje s p, potem je to število deljivo s p. Torej, p, $2\,p$, $3\,p, \ldots, p^{n-1}\,p^n$ so natanko števila na intervalu $[1, p^n]$, ki niso tuja s p. Takih števil je p^{n-1}. Ostalih $p^n - p^{n-1}$ pa je tujih s p.

Izrek 12 *Za poljubni tuji števili* $a, b \in \mathbb{N}$ *velja* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$*!*

Dokaz. Zapišimo števila od 1 do ab v tabeli:

$$\begin{array}{rrrcr} 1 & 2 & 3 & \cdots & a \\ a+1 & a+2 & a+3 & \cdots & 2a \\ 2a+1 & 2a+2 & 2a+3 & \cdots & 3a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (b-1)a+1 & (b-1)a+2 & (b-1)a+3 & \cdots & ba \end{array}$$

Števila, ki so tuja ab, morajo biti tuja a in tudi b. Oglejmo si po stolpcih, koliko je tujih z a in koliko z b.

Števila v k-tem stolpcu so oblike $i \cdot a + k$, kjer je $i = 0, \ldots, b-1$. Torej imajo vsa ta števila ostanek k pri deljenju z a. Zato sklepamo, da so bodisi vsa števila v nekem stolpcu tuja a bodisi nobeno ni tuje a. Stolpcev, ki vsebujejo števila, ki so tuja a, je $\varphi(a)$.....

Naloga 5 *Preveri zgornji izrek za* $\varphi(15) = \varphi(3) \cdot \varphi(5)$.

Posledica 13 *Naj bo* $n = p_1^{k_1}\, p_2^{k_2} \cdots p_r^{k_r}$ *praštevilski razcep števila* n*, kjer so* $p_1, p_2, \ldots, p_r$ *različna praštevila. Potem:*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Dokaz. Iz prejšnjega izreka sledi:

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{k_1})\,\varphi(p_2^{k_2}) \cdots \varphi(p_r^{k_r}) \\
&= (p_1^{k_1} - p_1^{k_1-1})\,(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) \\
&= p_1^{k_1}\,(1 - \tfrac{1}{p_1})\; p_2^{k_2}(1 - \tfrac{1}{p_2}) \;\cdots\; p_r^{k_r}(1 - \tfrac{1}{p_r}) \\
&= n\,(1 - \tfrac{1}{p_1})\,(1 - \tfrac{1}{p_2}) \cdots (1 - \tfrac{1}{p_r}).
\end{aligned}$$

□

Zgled:

$$\begin{aligned}
\varphi(720) &= \varphi(9 \cdot 8 \cdot 10) \\
&= \varphi(2^4)\varphi(3^2)\varphi(5) \\
&= (2^4 - 2^3) \cdot (3^2 - 3) \cdot (5 - 1) \\
&= 8 \cdot 6 \cdot 4 \\
&= 192
\end{aligned}$$

Izrek 14 *Za vsako naravno število* n *velja:*

$$\sum_{d \in D(n)} \varphi(d) = n\,.$$

Dokaz. Obravnavajmo množico

$$A = \left\{ \frac{k}{n}\,;\; 0 \leq k < n \right\}$$

Očitno je $|A| = n$. Zdaj okrajšamo vse ulomke iz A. Imenovalci dobljenih ulomkov so delitelji n. Števci ulomkov z imenovalcem d so števila tuja z d, takih ulomkov pa je $\varphi(d)$. Vseh ulomkov je torej

$$|A| = \left\{ \frac{k}{n}\,;\, 0 \leq k < n \right\} = \sum_{d \in D(n)} \varphi(d).$$

□

Zgled: Naj bo $n = 12$. Potem

$$\begin{aligned} A &= \{\tfrac{0}{12}, \tfrac{1}{12}, \tfrac{2}{12}, \tfrac{3}{12}, \tfrac{4}{12}, \tfrac{5}{12}, \tfrac{6}{12}, \tfrac{7}{12}, \tfrac{8}{12}, \tfrac{9}{12}, \tfrac{10}{12}, \tfrac{11}{12}\} \\ &= \{\tfrac{0}{1}, \tfrac{1}{12}, \tfrac{1}{6}, \tfrac{1}{4}, \tfrac{1}{3}, \tfrac{5}{12}, \tfrac{1}{2}, \tfrac{7}{12}, \tfrac{2}{3}, \tfrac{3}{4}, \tfrac{5}{6}, \tfrac{11}{12}\} \\ &= \{\tfrac{0}{1}, \tfrac{1}{2}, \tfrac{1}{3}, \tfrac{2}{3}, \tfrac{1}{4}, \tfrac{3}{4}, \tfrac{1}{6}, \tfrac{5}{6}, \tfrac{1}{12}, \tfrac{5}{12}, \tfrac{7}{12}, \tfrac{11}{12}\}. \end{aligned}$$

Sistemi s tajnim ključem

K je tajni ključ, ki ga poznata le pošiljatelj in prejemnik.

Imamo dva postopka, **kodiranje** $\mathcal{E}$ in **dekodiranje** $\mathcal{D}$, za katera velja:

- $\mathcal{E}(M, K) = C$;
- $\mathcal{D}(C, K) = M$;

kjer je M neko sporočilo in C ustrezni **kriptogram**.

Opomba. Pomanjkljivost je, da morata tajni ključ K poznati oba, tako pošiljatelj kot prejemnik!

Sistemi z javnim ključem

Pri sistemih z javnim ključem ima vsaka oseba X dva ključa:

- J_X je **javni ključ**, ki je znan vsem;
- T_X je **tajni ključ**, ki je znan samo lastniku.

Problem avtentikacije oz. digitalni podpis

Recimo, da oseba A želi poslati osebi B sporočilo M. Vprašanje je: kako bo B vedel, da je sporočilo zares poslal A! Uporabimo naslednji postopek:

1. Oseba A kodira sporočilo M s svojim tajnim ključem T_A ter tako dobi sporočilo $T_A(M)$. Potem kodira $T_A(M)$ z javnim ključem J_B ter dobi sporočilo $J_B(T_A(M))$.
2. Oseba B dekodira sporočilo $J_B(T_A(M))$ s tajnim ključem T_B ter dobi sporočilo $T_A(M)$. Potem dekodira $T_A(M)$ z javnim ključem J_A ter dobi začetno sporočilo M.

Kriptografska shema RSA

Ključa J_X in T_X dobimo takole:

1. izberimo različni veliki praštevili p in q;
2. izračunajmo: $n = p \cdot q$ in $m = (p-1) \cdot (q-1)$;
3. izberimo $1 < e < m$ tako, da je $e \perp m$;
4. z REA izračunajmo $1 < d < m$ tako, da je $d \cdot e \equiv 1 \pmod{m}$;
5. ključa sta $J_X = (n, e)$ in $T_X = d$.

Kodiramo in dekodiramo takole:

- **Kodiranje:** $C := M^e \pmod{n}$
- **Dekodiranje:** $M := C^d \pmod{n}$.

Da sta postopka kodiranja in dekodiranja usklajena, sledi iz naslednjega izreka:

Izrek 15 *Velja* $M^{de} \equiv M \pmod{n}$.

Dokaz. Za neko število k velja

$$de = km + 1 = k(p-1)(q-1) + 1.$$

Trdimo, da $M^{de} \equiv M \pmod{p}$. Če $p \mid M$, potem trditev očitno velja. Če pa $p \perp M$, potem $M \equiv 1 \pmod{p}$ in po Malem Fermatovem izreku sklepamo, da je $M^{p-1} \equiv 1 \pmod{p}$. Če potenciramo, dobimo $M^{k(p-1)(q-1)} \equiv 1 \pmod{p}$. Zdaj pa takoj sledi trditev.

Podobno dokažemo, da $M^{de} \equiv M \pmod{q}$.

Iz $p \mid M^{de} - M$ in $q \mid M^{de} - M$ sledi, da $pq \mid M^{de} - M$, kar je enako trditvi $M^{de} \equiv M \pmod{n}$. □