Euleri teoreem, Arvu järk, Astendamine, $\mathbf{a^n \pm 1}$

IMO treening

Oliver Nisumaa

13.06.17

Def. *Euleri funktsioon $\varphi(n)$ tähistab n-ga ühistegurita n jäägiklasside arvu.*

1. Näidata, et $\varphi(n)$ on nõrgalt multiplikatiivne, ehk kui $a \perp b$, siis $\varphi(ab) = \varphi(a)\varphi(b)$.
2. Näidata, et $\varphi\left(p^k\right) = p^k - p^{k-1}$, kus p on algarv.

Teoreem. *Euleri teoreem: Kui $a \perp m$, siis $a^{\varphi(m)} \equiv 1 (mod\ m)$*

3. Leia järgmiste arvude viimased numbrid

$$3^{1001}7^{1002}13^{1003} \text{ ja } 7^{7^{\cdot^{\cdot^{\cdot^{7}}}}} \text{ (mingi konkreetne arv astendamisi)}$$

4. (Kanada 2003) Leia järgmise arvu kolm viimast numbrit

$$2003^{2002^{2001}}$$

5. Olgu $p \geq 3$ algarv. Avaldame $p - 1 = 2^s d$, kus d on paaritu. Siis kas $a^d \equiv 1 (\text{mod } y)$ või $a^{2^r d} \equiv -1 (\text{mod } y)$ mingi $0 \leq r < s$ jaoks.

Seda tulemust kasutatakse Miller-Rabin algarvu testis.

6. (USAMO 1991) Näidata, et iga n jaoks on jada $2, 2^2, 2^{2^2}, \ldots (\text{mod } n)$ on lõpuks konstantne.

Def. *Kui $a \perp m$, nimetame arvu a järguks mooduli m järgi vähimat a astet n, mille korral $a^n \equiv 1 (mod\ m)$. Tähistatakse kas $ord_m(a)$ või lihtsalt $ord(a)$.*

7. $ord_m(a) \mid \varphi(m)$.

Def. *Ütleme, et g on algjuur mooduli m järgi, kui $ord_m(g) = \varphi(m)$.*

8. Kui m järgi leidub algjuur, siis neid on $\varphi(\varphi(m))$ tükki.

Teoreem. *Mooduli m järgi leidub algjuur, parajasti siis kui $m = 1, 2, 4, p^k, 2p^k$.*

9. Arv 5 on peaaegu algjuur 2^n järgi. $ord_{2^n}(5) = 2^{n-2}$. Avaldsed 5^k ja -5^k saavutavad kõik ühistegurita jäägiklassid mooduli 2^n järgi.

Def. *$m^n || a$ tähendab, et $m^n | a$ kuid $m^{n+1} \nmid a$*

10. $\gcd(a^n - 1, a^m - 1) = a^{\gcd(n,m)} - 1$
11. kui $a \equiv b \pmod{n}$, siis $a^n \equiv b^n \pmod{n^2}$.
12. $3^{k+1} || 2^{3^k} + 1$
13. $p | \binom{p}{k}$ kui $1 \leq k < p$
14. Olgu $a \geq 2$, $k \geq 1$, olgu $p \geq 3$ algarv, kui $p^k || a - 1$, siis $p^{k+1} || a^p - 1$

Teoreem. *Exponent lifting trick: Olgu $a \geq 2$, $k \geq 1$, $l \geq 0$ täisarvud, p olgu algarv. Kui $(p, k) \neq (2, 1)$ ning kehtib*

$$p^k || a - 1, \qquad p^l || n$$

Siis

$$p^{k+l} || a^n - 1$$

Erijuhul $n = p^l$ saame $p^{k+l} || a^{p^l} - 1$

15. 2 on algjuur mooduli 3^n järgi.

16. Kui g on algjuur mooduli p järgi ja $p^2 \nmid g^{p-1} - 1$, siis g on algjuur mooduli p^n ja $2p^n$ järgi iga n jaoks.

17. (IMO 1990) Leida kõik positiivsed täisarvud n, et $\dfrac{2^n + 1}{n^2}$ on täisarv.

18. (IMO 2000) Kas leidub positiivne täisarv N, mis jagub täpselt 2000 erineva algarvuga ja $2^N + 1$ jagub N-ga?

Veel arvuteooria ülesandeid:
104 Number Theory Problems.
http://yufeizhao.com/olympiad/exponent_lifting.pdf
http://yufeizhao.com/olympiad.html