Harjoitukset 4 / 2011 RATKAISUT Lukuteoria

1. *Osoita, että*
a) minkään kokonaisluvun neliö ei ole muotoa $4n+2$ *eikä* $4n+3$.
b) neljän peräkkäisen kokonaisluvun tulo on jaollinen luvulla 24.
c) k *peräkkäisen kokonaisluvun tulo on jaollinen kertomalla* $k!$.

a) Parillisen luvun neliö on muotoa $(2m)^2 = 4m^2 = 4n+0$, siis jakolaskualgoritmin mukaan ei muotoa $4n+2$ eikä $4n+3$. Parittoman luvun neliö on muotoa $(2m+1)^2 = 4m^2+4m+1$, siis jakolaskualgoritmin mukaan ei sekään muotoa $4n+2$ eikä $4n+3$.

Sama kongruenssein: Osoitetaaan, että 2 kertaluvun kongruensseilla $x^2 \equiv 2 \pmod 4$ ja $x^2 \equiv 3 \pmod 4$ ei ole ratkaisuja eli ratkaistaan 2. asteen yhtälöt $x^2 = 2$ ja $x^2 = 3$ renkaassa $\mathbb{Z}_4$. Ratkaiseminen on helppoa, koska on vain 4 vaihtoehtoa alkioksi $x \in \mathbb{Z}_4$, nimittäin luokat 0, 1, 2 ja 3. Koska $0^2 = 0$, $1^2 = 1$, $4^2 = 4 = 0$ ja $3^2 = 9 = 1$, ei ratkaisuja ole.

b) 4 peräkkäisistä luvuista kaksi on jaollisia 2:llä ja toinen niistä jopa 4:lla. Ainakin yksi on jaollinen 3:lla. Siis tulo on jaollinen $2 \cdot 4 \cdot 3 = 24$:lla.

c) k peräkkäisen **luonnollisen** luvun $a, a+1, \ldots a+k$ tulo on $\frac{(a+k)!}{a!}$ Jakamalla $k!$:lla saadaan luku $\frac{(a+k)!}{a!k!} = \binom{a+k}{a} = \binom{a+k}{k} \in \mathbb{N}$. Sillä asia on selvä. Jos taas alkuperäinen lukujono alkaa negatiivisesta luvusta, lisätään jokaiseen lukuun (sama) $mk!$ niin suurella m, että luvuista tulee positiiviisia. Tämä ei vaikuta laskuihin $\pmod{k!}$.

2. *Olkoon* $x \in \mathbb{R}$, $m \in \mathbb{N}$ *ja* $p \in \mathbb{P}$.
a) Osoita, että $\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor$
b) Osoita, että $p^{\lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \cdots} \mid m$, *mutta* $p^{1+\lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \cdots} \not| m$.
c) Kuinka moneen nollaan päättyy luvun 169! desimaaliesitys?
d) Osoita suoraan määritelmästä, että binomikertoimet $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ *ovat kokonaislukuja.*

a) Riittää osoittaa, ettei välillä $\left[\frac{\lfloor x \rfloor}{m}, \frac{x}{m} \right[$ ole yhtään kokonaislukua. Jos sellainen olisi vaikkapa n, niin nm olisi kokonaisluku välillä $[\lfloor x \rfloor, x[$, jolla ei ole kokonaislukuja.

b) Merkitään kanonisia esityksiä eli alkulukuhajoitelmia $k = \prod_{q \in \mathbb{P}} q^{a_q} \in \mathbb{N}$ jolloin tutkittavan alkuluvun p potenssi on

$$N_p(k) = N(k) = a_p = \max\{a \in \mathbb{N} \mid p \mid k\}.$$

Tehtävänä on laskea $N(m!)$.

Tietenkin $N(m!) = N(1 \cdot 2 \cdot 3 \cdot \cdots \cdot m = N(1) \cdot N(2) \cdot N(3) \cdot \cdots N(m)$, mutta koska p ei edes jaa muita jonon $1, 2, 3 \ldots$ lukuja kuin joka p:nnen, siis luvut $p, 2p, \ldots,$ niin

$$\begin{aligned} N(m!) &= N(p) \cdot N(2p) \cdot N(3p) \cdot \cdots \cdot N\left(\left\lfloor \frac{m}{p} \right\rfloor p\right) = N(p \cdot 2p \cdot 3p \cdot \cdots \cdot \left(\left\lfloor \frac{m}{p} \right\rfloor p\right)) \\ &= N(p^{\left\lfloor \frac{m}{p} \right\rfloor} \cdot 1 \cdot 2 \cdot 3 \cdot \cdots \cdot \left\lfloor \frac{m}{p} \right\rfloor) = \left\lfloor \frac{m}{p} \right\rfloor + N(1 \cdot 2 \cdot 3 \cdot \cdots \cdot \left\lfloor \frac{m}{p} \right\rfloor) \\ &= \left\lfloor \frac{m}{p} \right\rfloor + N\left(\left\lfloor \frac{m}{p} \right\rfloor\right)! \end{aligned}$$

Tätä menettelyä voi toistaa! Tulokseksi saadaan a)-kohdan perusteella

$$N(m!) = \left\lfloor \frac{m}{p} \right\rfloor + N\left(\left\lfloor \frac{m}{p} \right\rfloor \right)! = \left\lfloor \frac{m}{p} \right\rfloor + \lfloor \frac{\left\lfloor \frac{m}{p} \right\rfloor}{p} \rfloor + N(\lfloor \frac{\left\lfloor \frac{m}{p} \right\rfloor}{p} \rfloor)$$
$$= \lfloor \tfrac{m}{p} \rfloor + \lfloor \tfrac{m}{p^2} \rfloor + N(\lfloor \tfrac{m}{p^2} \rfloor) = \cdots = \lfloor \tfrac{m}{p} \rfloor + \lfloor \tfrac{m}{p^2} \rfloor + \lfloor \tfrac{m}{p^3} \rfloor + \ldots \text{ äärellinen summa.}$$

c) Kuinka moneen nollaan päättyy luvun 169! desimaaliesitys? Tämä on melkein suora sovellus b)-kohdasta. Olkoon siis m=169. Koska 10 ei ole alkuluku, täytyy tietenkin tutkia erikseen sen alkutekijät 5 ja 2. Olkoon siis ensin $p = 2$ (osoittautuu huonoksi järjestykseksi).

$$N_2(169!) = \lfloor \tfrac{169}{2} \rfloor + \lfloor \tfrac{169}{2^2} \rfloor + \lfloor \tfrac{169}{2^3} \rfloor + \cdots =$$
$$= 84 + 42 + 21 + 10 + 5 + 2 + 1.$$

Olkoon sitten $p = 5$

$$N_5(169!) = \lfloor \tfrac{169}{5} \rfloor + \lfloor \tfrac{169}{5^2} \rfloor + \lfloor \tfrac{169}{5^3} \rfloor + \cdots =$$
$$= 33 + 6 + 1 = 40.$$

Koska jälkimmäinen (tietysti!) on pienempi, on 169! jaollinen 10:llä 40 kertaa.

d) Binomikertoimet $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ ovat kokonaislukuja, koska b)-kohdan kaavan mukaan jokainan nimittäjän alkutekijä esiintyy osoittajassa vähintään yhtä monta kertaa kuin nimittäjässä.

3. ...

Etsi käänteiset

a) Katsomalla kertomataulua mod 11-silmällä huomaa, että luvuille $1 \ldots 10$ käänteiset $\pmod{11}$ ovat (järjestyksessä) $1, 6, 4, 3, 9, 2, 8, 7, 5$

b) Luvuille $-12 \ldots 12 \pmod{12}$ Luvuista 1–12 ainoastaan $\varphi(12) = kpl$ ovat kääntyviä mod 12 eli suhteellisisa alkulukuja 12 kanssa, nimittäin luvut 1,5,7 ja 11. Katsomalla kertomataulua mod 12-mielessä huomaa, että luvuille 1,5,7 ja 11 käänteiset (mod 12) ovat (järjestyksessä) 1,5,7,11, siis kaikii itsensä käänteisiä.

Helpommalla pääsee valitsemalla käännettäviksi luvut 1,5,7-12=-5 ja 11-12=-1, joiden käänteiset ovat 1,5,-5 ja -1.

Täsmällinen vastaus kysymykseen on siis....

4. ....

7:n jaollisuusääntö saadaan suoraan desimaaliesityksestä:

$$N = \sum_j a_j 10^j$$
$$\equiv a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + a_4 \cdot 10^4 + \ldots$$
$$\equiv a_0 + a_1 \cdot 3 + a_2 \cdot 3^2 + a_3 \cdot 3^3 + a_4 \cdot 3^4 + \ldots$$
$$\equiv a_0 + a_1 \cdot 3 + a_2 \cdot 2 + a_3 \cdot (-1) + a_4 \cdot 3 \cdot (-1) + a_5 \cdot 2 \cdot (-1) + \ldots$$
$$\equiv (a_0 + a_1 \cdot 3 + a_2 \cdot 2) - (a_3 + a_4 \cdot 3 + a_5 \cdot 2) + \ldots \pmod{7}$$

$$7 \mid n = \prod a_\mu 10^\mu \iff 7 \mid (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + (a_6 + 3a_7 + 2a_8) - \ldots$$

5. ...

a) Kirjoitan näkyviin kaksi täydellistä (tjs) ja kaksi ja supistettua (sjs) jäännössysteemiä $\pmod{20}$.

$\{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19\}$

ja $\{-1,0,1,2,3,4,5,6,7,8,9,11,12,13,14,15,16,17,18,20000000000010\}$ ovat tjs.

$1,3,7,9,11,13,17,19$ on sjs, samoin $-9,-7,-3,-1,1,3,7,9$. (Huomaa lukumäärä $\varphi(20)=\varphi(5)\cdot\varphi(4)=4\cdot 2=8$ ja jälkimmäisen symmetria.)

b) Täydellinen jäännössysteemi (tjs) modulo n on $\{1,2,\ldots,n\}$ (1-käsitteiset luvut mod n), joten $2\cdot\sum(tjs.)=n(n+1)\equiv 0$. Pienin positiiviluku x, joka toteuttaa kongruenssin $2x\equiv 0 \pmod{n}$ on $n/2$, jos n on parillinen ja n muuten.

c) Jos $n>2$, niin supistettu jäännössysteemi (sjs) modulo n on kirjoitettavissa muotoon $\{-a_1,\ldots,-a_m,a_m,\cdots-a_1\}$, sillä $(k,n)=(-k,n)$ Siis $\sum(sjs.)\equiv 0$, joten etsitty luku on n. Erikoistapauksessa $n=2$ on sjs=$\{1\}$, jonka pienin positiivinen edustaja eli etsitty luku on 1.

6. ...

a) Olkoon $(m,n)=1$. Väite sanoo, että kun x käy läpi tjs:n $\pmod{m}$ (olkoon se X) ja y käy tjs:n $\pmod{n}$ (olkoon se Y), niin luvut $xn+ym$ käyvät t.j.s:n $\pmod{mn}$, toisin sanoen niitä on mn kappaletta ja ne ovat parittain epäkongruentteja $\pmod{nm}$. Osoitetaan ensin epäkongruenttisuus. Jos kuitenkin olisi

$$x_1n+y_1m\equiv x_2n+y_2m \pmod{nm},$$

niin, koska $(n,m)=1 \implies n$ on kääntyvä renkaassa $\mathbb{Z}_m$,

$$\begin{aligned}
x_1n+y_1m &\equiv x_2n+y_2m \pmod{nm}\\
(x_1-x_2)n &\equiv (y_2-y_1)m \pmod{nm}\\
(x_1-x_2)n &\equiv (y_2-y_1)m\equiv 0 \pmod{m} \quad \Big| \cdot n'\\
(x_1-x_2) &\equiv 0 \pmod{m}\\
x_1 &\equiv x_2 \pmod{m}\\
x_1 &= x_2 \pmod{m},\ \text{koska } x_1,x_2\in X,\ \text{joka on tjs}
\end{aligned}$$

Vastaavasti $y_1=y_2$. Koska siis luvut $xn+ym$ ovat parittain epäkongruentteja, niitä on mös oikea määrä eli nm kpl.

b) aivan samanlainen lasku, mutta on lisäksi osoitettava, että $xn+ym$ kuuluu sjs:ään eli on alkuluokka $\pmod{mn}$ eli kääntyvä renkaassa $\mathbb{Z}_{mn}$, kun x on alkuluokka $\pmod{n}$, y on alkuluokka $\pmod{m}$ ja $(m,n)=1$. Osoitetaan, että $(xn+ym,nm)=1$. Koska $(n,m)=1$, tämä on yhtäpitävää sen kanssa, että $(xn+ym,n)=1$ ja $(xn+ym,m)=1$. Selvästi $(xn+ym,n)=(ym,n)=1$, koska sekä y että n ovat oletuksen mukaan suhteellisisa alkulukuja m:n kanssa. Vastaavasti $(xn+ym,m)=1$. $\square$.

7. **Millerin testi.** *Luku n, jolle $n-1=2^st$, (t pariton), läpäisee Millerin testin kantaluvun a suhteen, jos joko*

$$a^t\equiv 1 \pmod{n} \tag{1}$$

tai

$$a^{2^jt}\equiv -1 \pmod{n} \quad \textit{jollakin } 0\le j\le s-1. \tag{2}$$

Wikipedia

Just like the Fermat and Solovay–Strassen tests, the Miller–Rabin test relies on an equality or set of equalities that hold true for prime values, then checks whether or not they hold for a number that we want to test for primality.

First, a lemma about square roots of unity in the finite field Z_p, where p is prime and $p > 2$. Certainly 1 and -1 always yield 1 when squared mod p; call these **trivial** square roots of 1.

Lemma: There are no nontrivial square roots of 1 mod p

Proof. This is a a special case of the result that, in a field, a polynomial has no more zeroes than its degree. To show this directly, suppose that x is a square root of 1 mod p. Then: $x^2 \equiv 1 \pmod{p}$ ie. $(x-1)(x+1) \equiv 0 \pmod{p}$, which in a field implies $(x+1) \equiv 0 \pmod{p}$ or $(x-1) \equiv 0 \pmod{p}$. □

Päätodistus:Now, let p be an odd prime. Then $p-1$ is even and we can write it as $2^s \cdot d$, where s and d are positive integers, and d is odd. For each $a \in \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$, either

$$a^d \equiv 1 \pmod{p}$$

or

$$a^{2^r d} \equiv -1 \pmod{p}$$

for some $0 \leq r < s$.

To show that one of these must be true, recall **Fermat's little theorem**: (Kantaluku a valitaan niin, ettei se ole p:n monikerta.)

$$a^{p-1} \equiv 1 \pmod{p}$$

By the lemma above, if we keep taking square roots of a^{p-1}, we will get either 1 or -1. If we get -1 then the second equality holds and we are done. If we never get -1, then when we have taken out every power of 2, we are left with the first equality. □

Mathematica versions 2.2 and later have implemented the multiple Rabin-Miller test in bases 2 and 3 combined with a Lucas pseudoprime test as the primality test used by the function PrimeQ[n]. As of 1997 no counterexamples are known and if any exist, they are expected to occur with extremely small probability (i.e., much less than the probability of a hardware error on a computer performing the test).

8. *Ratkaise kongruenssi* $x^2 \equiv -1 \pmod{13}$ *Wilsonin lauseen avulla.*

13 on alkuluku. Siten Wilsonin lause antaa

$$(13-1)! + 1 \equiv 0 \pmod{13}$$

eli

$$12! \equiv -1 \pmod{13}.$$

Huomataan, että

$$\begin{aligned} 12 &\equiv -1 \pmod{13} \\ 11 &\equiv -2 \pmod{13} \\ 10 &\equiv -3 \pmod{13} \\ &\vdots \\ 7 &\equiv -6 \pmod{13}. \end{aligned}$$

Siis $-1 \equiv 12! \equiv (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6)^2 \equiv 24^2 \equiv 5^2 \pmod{13}$. Tietysti myös -5 on ratkaisu!.