Lukuteorian kertausta ja syvennystä

Tehtäviä jaollisuudesta

1. Olkoot a, b, c ja d kokonaislukuja, joille $a \neq c$ ja $(a-c) \mid (ab+cd)$. Osoita, että $(a-c) \mid (ad+bc)$.

2. Olkoon n pariton positiivinen kokonaisluku. Osoita, että $24 \mid (n^3 - n)$.

3. Olkoon p alkuluku, jolle myös p^2+2 on alkuluku. Osoita, että tällöin myös p^3+2 on alkuluku.

4. Mitä p voi olla, jos p, $p+10$ ja $p+14$ ovat kaikki alkulukuja?

5. Olkoon p alkuluku. Etsi kaikki positiiviset kokonaisluvut x ja y, joille

$$x^2 - y^2 = p.$$

6. Olkoon p alkuluku. Etsi kaikki positiiviset kokonaisluvut x ja y, joille

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{p}.$$

7. Etsi kaikki positiiviset kokonaisluvut x, y ja z, joille

$$4xy - x - y = z^2.$$

8. Etsi kaikki positiiviset kokonaisluvut x, y, joille

$$y^2 = x^3 + 7.$$

9. Osoita, että positiivisella kokonaisluvulla n on pariton määrä tekijöitä jos ja vain jos n on neliöluku.

10. Olkoon a positiivinen kokonaisluku, jolle $2^a - 1$ on alkuluku. Osoita, että tällöin $2^{n-1}(2^n - 1)$ on täydellinen luku.

11. Todista seuraava seitsemällä jaollisuussääntö: Olkoon n vähintään kolminumeroinen positiivinen kokonaisluku, jonka viimeinen numero on d. Lasketaan $m = (n-d)/10 - 2d$. Tällöin $7 \mid n$ jos ja vain jos $7 \mid m$.

12. Voiko neliöluvun numeroiden summa olla 1977?

Kongruenssit

13. Olkoon m positiivinen kokonaisluku, ja olkoon P kokonaislukukertoiminen polynomi. Osoita, että jos kokonaisluvuille x ja y pätee $x \equiv y \pmod{m}$, niin myös $P(x) \equiv P(y) \pmod{m}$. Osoita lisäksi, että jos $x \neq y$, niin pätee myös $(x-y) \mid (P(x) - P(y))$.

14. Olkoon p pariton alkuluku, ja olkoot $x_1, x_2, \ldots, x_p$ kokonaislukuja, joille

$$x_1^{p-1} + x_2^{p-1} + \ldots + x_p^{p-1} \equiv 0 \pmod{p}.$$

Osoita, että tällöin $x_k \equiv x_\ell \pmod{p}$ joillakin $k, \ell \in \{1, 2, \ldots, p\}$, joille $k \neq \ell$.

15. Olkoot P ja Q kokonaislukukertoimisia polynomeja, joille $P(1000) = 1000$, $P(2001) = 2000$ ja $Q(0) = 5$. Etsi kaikki kokonaislukuratkaisut x yhtälölle $Q(P(x)) = 0$.

16. Etsi kokonaisluvut n, joille $\varphi(n) = n/2$.

17. Olkoon n positiivinen kokonaisluku. Osoita, että on olemassa n peräkkäistä kokonaislukua, joista jokainen on jaollinen ainakin kahdella eri alkuluvulla.

18. Olkoon p pariton alkuluku. Mitä ovat

$$1^2 \cdot 3^2 \cdot 5^2 \cdot \ldots \cdot (p-2)^2 \quad \text{ja} \quad 2^2 \cdot 4^2 \cdot 6^2 \cdot \ldots \cdot (p-1)^2$$

modulo p?

19. Olkoon p pariton alkuluku. Osoita, että jos $p \equiv 1 \pmod 4$, niin

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod p,$$

ja että jos $p \equiv -1 \pmod 4$, niin

$$\left(\frac{p-1}{2}\right)! \equiv 1 \quad \text{tai} \quad -1 \pmod p.$$

Joidenkin yhtälöiden kokonaislukuratkaisuista

20. Osoita, että yhtälöllä

$$x^3 + y^3 + z^3 = 3^n$$

on kokonaislukuratkaisu jokaisella positiivisella kokonaisluvulla n.

21. Etsi kaikki positiiviset kokonaisluvut x ja y, joille

$$x^3 + y^4 = 7.$$

22. Olkoon p alkuluku, ja olkoon $p \neq 3$. Etsi kaikki positiiviset kokonaisluvut x, y ja z, joille

$$x^3 + 3y^3 + 9z^3 - 3pxyz = 0.$$

23. Etsi kaikki positiiviset kokonaisluvut x, y ja z, joille

$$x^2 + y^2 + z^2 - 2xyz = 0.$$

24. Etsi kaikki positiiviset kokonaisluvut x ja y, joille

$$x^6 + 3x^3 + 1 = y^4.$$

25. Etsi kaikki positiiviset kokonaisluvut x ja y, joille

$$x(x+1)(x+2)(x+3) = y^4.$$

Vihjeitä

1. Tarkastele lukujen $ad + bc$ ja $ab + cd$ erotusta.

2. Totea, että $n^3 = (n-1)\,n\,(n+1)$.

3. Tarkastele ensin tapausta $p \neq 3$. Mitä $p^2 + 2$ on modulo 3?

4. Tarkastele lukuja modulo 3.

5. Kirjoita $x^2 - y^2 = (x+y)\,(x-y)$, ja hyödynnä yksikäsitteistä tekijöihinjakoa.

6. Yhtälön voi kirjoittaa muodossa $(x-p)\,(y-p) = p^2$, ja jälleen yksikäsitteinen tekijöihinjako on hyödyllinen.

7. Muokkaa yhtälöä niin, että vasen puoli täydentyy tuloksi $(4x-1)\,(4y-1)$. Tässä on hyödyllistä tietää, että jos q on alkuluku, jolle $q \equiv 3 \pmod 4$, niin -1 ei ole neliönjäännös modulo q.

8. Tässä on luonnollista aloittaa kirjoittamalla yhtälö muodossa $y^2 + 1 = x^3 + 8$. Jaa oikea puoli tekijöihin ja käsittele erikseen tapauksia $2 \mid x$ ja $2 \nmid x$. Tapauksessa $2 \nmid x$ tarkastele oikean puolen toisen asteen tekijää, ja muista, milloin -1 on neliönjäännös modulo alkuluku.

9. Jos luvun $n > 1$ alkutekijähajotelma on

$$n = \prod_{\ell=1}^{r} p_\ell^{\alpha_\ell}, \quad \text{niin} \quad d(n) = \prod_{\ell=1}^{r} (\alpha_\ell + 1)\,.$$

10. Luvun n sanotaan olevan täydellinen, jos $\sigma(n) = 2n$. Jos luvun $n > 1$ alkutekijähajotelma on

$$n = \prod_{\ell=1}^{r} p_\ell^{\alpha_\ell}, \quad \text{niin} \quad \sigma(n) = \prod_{\ell=1}^{r} \left(1 + p_\ell + p_\ell^2 + \ldots + p_\ell^{\alpha_\ell}\right) = \prod_{\ell=1}^{r} \frac{p_\ell^{\alpha_\ell+1} - 1}{p_\ell - 1}.$$

11. Tarkastele suoraan kongruenssia $m \equiv 0 \pmod 7$, ja yritä johtaa siitä $n \equiv 0 \pmod 7$, ja kääntäen.

12. Kolmella ja yhdeksällä jaollisuussäännöt ovat tässä molemmat hyödyllisiä.

13. Jos $x \equiv y \pmod m$, niin myös $x^2 \equiv y^2 \pmod m$, $x^3 \equiv y^3 \pmod m$, ...

14. Fermat'n pienen lauseen nojalla $x^{p-1} \equiv 1 \pmod p$, kun x on kokonaisluku, jolle $x \not\equiv 0 \pmod p$.

15. Jos kokonaisluvuille x ja y pätee $x \equiv y \pmod 2$, niin myös $P(x) \equiv P(y) \pmod 2$.

16. Jos luvun $n > 1$ alkutekijähajotelma on

$$n = \prod_{\ell=1}^{r} p_\ell^{\alpha_\ell}, \quad \text{niin} \quad \varphi(n) = n \prod_{\ell=1}^{r} \frac{p_\ell - 1}{p_\ell}.$$

17. Kokeile kiinalaista jäännöslausetta niin, että moduluksina on sopivia kahden eri alkuluvun tuloja.

18. Wilsonin lause on tässä hyödyllinen, samoin kuin havainto, että kaikille kokonaisluvuille k pätee $k \equiv (-1)\,(p-k) \pmod{p}$.

19. Wilsonin lause on tässä hyödyllinen, samoin kuin havainto, että kaikille kokonaisluvuille k pätee $k \equiv (-1)\,(p-k) \pmod{p}$.

20. Totea, että riittää tarkastella tapauksia $n \in \{0, 1, 2\}$.

21. Mitä tapahtuu, jos tarkastelet yhtälöä modulo 13?

22. Totea ensin, että $3 \mid x$, seuraavaksi, että $3 \mid y$, ja sitten, että $3 \mid z$. Voiko tässä toteuttaa äärettömän laskeutumisen?

23. Totea ensin, etteivät kaikki tuntemattomat voi olla parittomia. Totea sitten, että $x^2+y^2+z^2 \equiv 0 \pmod{4}$. Mitä tästä seuraa lukujen x, y ja z parillisuudelle? Voisiko tässä toteuttaa äärettömän laskeutumisen?

24. Millaisia lukuja ovat x^6, $(x^3+1)^2$ ja $(x^3+2)^2$?

25. Millaisia lukuja ovat x^4, $(x+1)^4$ ja $(x+2)^4$?

Ratkaisuita

1. Aloitetaan toteamalla, että

$$(ad+bc)-(ab+cd) = ad-cd-ab+cb = (a-c)\,d+(c-a)\,b = (a-c)\,(d-b)\,.$$

Tämän vuoksi, jos toinen luvuista $ad+bc$ ja $ab+cd$ on jaollinen luvulla $a-c$, niin myös toisenkin on oltava.

2. Todetaan ensin, että $n^3-n = (n-1)\,n\,(n+1)$. Koska tässä on kolme peräkkäistä kokonaislukua, jonkin niistä on oltava jaollinen kolmella. Toisaalta, koska n on pariton, niin luvut $n\pm 1$ ovat parillisia, ja peräkkäisinä parillisina lukuina toinen niistä on jaolinen neljällä. Yhdistämällä nämä havainnot saadaan

$$24 = 2\cdot 3\cdot 4 \mid (n-1)\,n\,(n+1) = n^3-n.$$

3. Jos $p\neq 3$, niin $p\equiv \pm 1 \pmod 3$, ja edelleen $p^2+2\equiv 1+2\equiv 0 \pmod 3$. Mutta toisaalta $p^2+2\geqslant 2^2+2>3$, eli nyt p^2+2 ei voisikaan olla alkuluku. Siis ainoa mahdollisuus on $p=3$, jolloin $p^2+2=11$ ja $p^3+2=29$ ovat molemmat alkulukuja.

4. Modulo kolme kyseiset luvut ovat

$$p\equiv p, \quad p+10\equiv p+1, \quad \text{ja} \quad p+14\equiv p+2 \pmod 3.$$

Siispä jokin luvuista p, $p+10$ ja $p+12$ on kolmella jaollinen. Koska $p+14>p+10>3$, voi olla ainoastaan $p=3$. Tällöin $p+10=13$ ja $p+14=17$ ovat alkulukuja, eli $p=3$ tosiaan on mahdollinen arvo.

5. Yhtälöstä seuraa, että

$$(x+y)\,(x-y) = p.$$

Koska $x+y>0$ ja $p>0$, on myös $x-y>0$. Siis $x>y$ ja $x\pm y$ ovat luvun p positiivisia tekijöitä. Koska luvun p ainoat positiiviset tekijät ovat 1 ja p, voi olla ainoastaan

$$x+y=p, \quad \text{ja} \quad x-y=1.$$

Tällä yhtälöparilla on täsmälleen yksi rationaalinen ratkaisu, nimittäin

$$x=\frac{p+1}{2}, \quad \text{ja} \quad y=\frac{p-1}{2}.$$

Tämä on kokonaislukuratkaisu täsmälleen silloin kun p on pariton.

6. Lavennetaan ja kerrotaan kaikki auki, jolloin saadaan ensin

$$p\,(x+y) = xy, \quad \text{ja sitten} \quad (x-p)\,(y-p) = p^2.$$

Nyt $x-p$ on luvun p^2 tekijä ja voi olla vain ja ainoastaan p^2, p, 1, -1, $-p$ tai $-p^2$, jolloin tekijän $y-p$ täytyy vastaavasti olla 1, p, p^2, $-p^2$, $-p$ tai -1. Yhtälöparien

$$\begin{cases} x-p=p^2, \\ y-p=1, \end{cases} \quad \begin{cases} x-p=p, \\ y-p=p, \end{cases} \quad \begin{cases} x-p=1, \\ y-p=p^2, \end{cases}$$

$$\begin{cases} x-p=-1, \\ y-p=-p^2, \end{cases} \quad \begin{cases} x-p=-p, \\ y-p=-p, \end{cases}, \quad \text{ja} \quad \begin{cases} x-p=-p^2, \\ y-p=-1, \end{cases}$$

ratkaisut ovat

$$\begin{cases} x = p^2 + p, \\ y = p + 1, \end{cases} \quad \begin{cases} x = 2p, \\ y = 2p, \end{cases} \quad \begin{cases} x = p + 1, \\ y = p^2 + p, \end{cases} \quad \begin{cases} x = p - 1, \\ y = p - p^2, \end{cases} \quad \begin{cases} x = 0, \\ y = 0, \end{cases} \quad \begin{cases} x = p - p^2, \\ y = p - 1, \end{cases}$$

joista ainoastaan kolme ensimmäistä ovat positiivisia kokonaislukuratkaisuita.

7. Kirjoitetaan yhtälö muodossa

$$(4x - 1)(4y - 1) = (2z)^2 + 1.$$

Vasemman puolen tekijä $4x - 1$ on varmasti positiivinen ja pariton. Sen kaikki alkulukutekijät q ovat $\equiv \pm 1 \pmod 4$. Jos ne kaikki olisivat $\equiv 1 \pmod 4$, olisi myös $4x - 1$ tällaisten lukujen tulona $\equiv 1 \pmod 4$, mitä se ei ole. Siispä luvulla $4x - 1$ on ainakin yksi alkulukutekijä q, jolle $q \equiv -1 \pmod 4$. Mutta nyt

$$q \mid \left((2z)^2 + 1\right), \quad \text{eli} \quad -1 \equiv (2z)^2 \pmod q,$$

mikä on mahdotonta. Täten halutunlaisia ratkaisuita ei ole.

8. Todetaan ensin, että jos x on parillinen, niin

$$y^2 \equiv x^3 + 7 \equiv 0 + 3 \equiv 3 \pmod 4,$$

mikä on mahdotonta. Siis on oltava $2 \nmid x$, eli $x \equiv \pm 1 \pmod 4$. Yhtälöstä seuraa, että

$$y^2 + 1 = x^3 + 8 = x^3 + 2^3 = (x + 2)\left(x^2 - 2x + 4\right).$$

Ensinnäkin

$$x^2 - 2x + 4 = (x - 1)^2 + 3 > 0,$$

ja toisaalta

$$x^2 - 2x + 4 \equiv 1 \mp 2 + 4 \equiv -1 \pmod 4.$$

Tekijä $x^2 - 2x + 4$ on siis positiivinen ja pariton, ja sen kaikki alkulukutekijät ovat $\equiv \pm 1 \pmod 4$. Jos ne kaikki olisivat $\equiv 1 \pmod 4$, niin myös $x^2 - 2x + 4$ olisi sellaisten lukujen tulona $\equiv 1 \pmod 4$, mitä se ei ole. Siispä luvulla $x^2 - 2x + 4$ on oltava ainakin yksi alkulukutekijä q, jolle $q \equiv -1 \pmod 4$. Mutta nyt

$$q \mid \left(y^2 + 1\right), \quad \text{eli} \quad -1 \equiv y^2 \pmod q,$$

mikä on mahdotonta.

9. Todetaan ensiksi, että $n = 1^2$ vain ja ainoastaan silloin kun $d(n) = 1$. Voimme siis tarkastella tilannetta, missä $n > 1$ ja $d(n) > 1$. Olkoon luvun n kanoninen alkutekijähajotelma

$$n = \prod_{\ell=1}^{r} p_\ell^{\alpha_\ell},$$

missä $r \in \mathbb{Z}_+$, $p_1 < p_2 < \ldots < p_r$ ovat eri alkulukuja ja eksponentit $\alpha_1, \alpha_2, \ldots, \alpha_r$ ovat positiivisia kokonaislukuja. Tällöin luvun tekijöiden lukumäärä on

$$d(n) = \prod_{\ell=1}^{r} (\alpha_\ell + 1).$$

Tämä tulo on pariton jos ja vain jos sen jokainen tulontekijä on pariton. Toisin sanoen, $2 \nmid d(n)$ täsmälleen silloin kun eksponenteista $\alpha_1, \alpha_2, \ldots, \alpha_r$ jokainen on parillinen, mikä taas puolestaan pitää paikkaansa täsmälleen silloin kun n on neliöluku.

10. Olkoon kokonaisluvun $n > 1$ kanoninen alkutekijähajotelma

$$n = \prod_{\ell=1}^{r} p_\ell^{\alpha_\ell},$$

missä $r \in \mathbb{Z}_+$, $p_1 < p_2 < \ldots < p_r$ ovat eri alkulukuja, ja eksponentit α_1, α_2, $\ldots$, α_r ovat positiivisia kokonaislukuja. Tällöin luvun n tekijöiden summa on

$$\sigma(n) = \prod_{\ell=1}^{r} \left(1 + p_\ell + p_\ell^2 + \ldots + p_\ell^{\alpha_\ell}\right) = \prod_{\ell=1}^{r} \frac{p_\ell^{\alpha_\ell+1} - 1}{p_\ell - 1}.$$

Erityisesti, jos $a \in \mathbb{Z}_+$ on sellainen, että $2^a - 1$ on alkuluku, niin kyseessä on pariton alkuluku. Voimme sitten laskea suoraan, että

$$\sigma\big(2^{a-1}\,(2^a - 1)\big) = \frac{2^{a-1+1} - 1}{2 - 1} \cdot (1 + 2^a - 1) = (2^a - 1) \cdot 2^a = 2 \cdot 2^{a-1}\,(2^a - 1)\,.$$

11. Jos $m \equiv 0 \pmod 7$, niin $(n - d)/10 \equiv 2d \pmod 7$. Kertomalla puolittain luvulla 10 tästä seuraa, että $n - d \equiv 20d \pmod 7$, eli $n \equiv 21d \equiv 0 \pmod 7$.

Kääntäen, jos $n \equiv 0 \pmod 7$, niin $n \equiv 21d \pmod 7$, ja $n - d \equiv 20d \pmod 7$. Kertomalla puolittain luvulla 5 saadaan

$$\frac{n - d}{10} \equiv 5 \cdot 10 \cdot \frac{n - d}{10} \equiv 5\,(n - d) \equiv 100d \equiv 2d \pmod 7,$$

mistä seuraa, että $m \equiv 0 \pmod 7$, kuten pitääkin.

12. Merkitään positiivisen kokonaisluvun n numeroiden summaa $s(n)$. Tunnetusti $n \equiv s(n) \pmod 3$ ja $n \equiv s(n) \pmod 9$. Jos nyt olisi $s(a^2) = 1977$ jollakin positiivisella kokonaisluvulla a, niin koska $3 \mid 1977$, olisi $3 \mid a^2$. Edelleen, olisi $3 \mid a$ ja $9 \mid a^2$, ja olisi oltava $9 \mid 1977$. Mutta itse asiassa $9 \nmid 1977$. Siis neliöluvun numeroiden summa ei koskaan voi olla 1977.

13. Olkoon polynomi $P(x)$ vaikkapa

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0,$$

missä $n \in \mathbb{Z}_+ \cup \{0\}$ ja a_0, a_1, $\ldots$, a_n ovat kokonaislukuja. Nyt

$$\left.\begin{array}{rcl} 1 \equiv 1 & & a_0 \equiv a_0 \\ x \equiv y & & a_1 x \equiv a_1 y \\ x^2 \equiv y^2 & & a_2 x^2 \equiv a_2 y^2 \\ \vdots & \text{ja edelleen} & \vdots \\ x^{n-1} \equiv y^{n-1} & & a_{n-1} x^{n-1} \equiv a_{n-1} y^{n-1} \\ x^n \equiv y^n & & a_n x^n \equiv a^n y^n \end{array}\right\} \pmod m.$$

Laskemalla nämä viimeiset kongruenssit yhteen saadaan $P(x) \equiv P(y) \pmod m$. Jos $x \neq y$, niin sijoittamalla $m = |x - y|$ nähdään, että $P(x) \equiv P(y) \pmod{(x - y)}$, sillä onhan varmasti $x \equiv y \pmod{(x - y)}$.

14. Tehdään vastaoletus: oletetaan, että luvut x_1, x_2, $\ldots$, x_p ovat pareittain epäkongruentteja modulo p. Tällöin jokainen niistä on kongruentti täsmälleen yhden luvuista 1, 2, $\ldots$, p kanssa modulo p, ja kääntäen. Mutta nyt Fermat'n pienen lauseen nojalla

$$x_1^{p-1} + x_2^{p-1} + \ldots + x_{p-1}^{p-1} + x_p^{p-1} \equiv 1 + 1 + \ldots + 1 + 0 \equiv p - 1 \not\equiv 0 \pmod p,$$

vastoin tehtävänannon oletuksia.

15. Tunnetusti $P(x) \equiv P(y) \pmod 2$ aina kun kokonaisluvuille x ja y pätee $x \equiv y \pmod 2$. Jos $x \equiv 0 \pmod 2$, niin $x \equiv 1000 \pmod 2$, ja

$$P(x) \equiv P(1000) = 1000 \equiv 0 \pmod 2.$$

Jos taas $x \equiv 1 \pmod 2$, niin $x \equiv 2001 \pmod 2$, ja

$$P(x) \equiv P(2001) = 2000 \equiv 0 \pmod 2.$$

Siis kaikilla $x \in \mathbb{Z}$ pätee $P(x) \equiv 0 \pmod 2$. Siirtymällä nyt tarkastelemaan polynomin Q arvoja, tästä seuraa, että kaikilla $x \in \mathbb{Z}$ pätee

$$Q(P(x)) \equiv Q(0) = 5 \equiv 1 \not\equiv 0 \pmod 2,$$

eli kaikki lausekkeen $Q(P(x))$ arvot ovat parittomia eikä yhtälöllä $Q(P(x)) = 0$ voi olla kokonaislukuratkaisuita.

16. Koska $\varphi(n)$ on kokonaisluku, on oltava $2 \mid n$. Jos $n = 2^\alpha$, missä $\alpha \in \mathbb{Z}_+$, niin

$$\varphi(n) = 2^\alpha \cdot \frac{2-1}{2} = \frac{2^\alpha}{2},$$

eli luvun kaksi potenssit ovat halutunlaisia lukuja. Oletetaan sitten, että n on parillinen mutta ei luvun kaksi potenssi.

Olkoon luvun n kanoninen alkutekijähajotelma

$$n = \prod_{\ell=1}^{r} p_\ell^{\alpha_\ell},$$

missä $r \in \mathbb{Z}_+$, $r \geqslant 2$, $2 = p_1 < p_2 < \ldots < p_r$ ovat eri alkulukuja, ja eksponentit $\alpha_1, \alpha_2, \ldots, \alpha_r$ ovat positiivisia kokonaislukuja. Tunnetusti

$$\varphi(n) = n \prod_{\ell=1}^{r} \frac{p_\ell - 1}{p_\ell}.$$

Yhtälön $\varphi(n) = n/2$ voi kirjoittaa nyt muotoon

$$2^{\alpha_1} \cdot \frac{2-1}{2} \cdot \prod_{\ell=2}^{r} p_\ell^{\alpha_\ell} \cdot \frac{p_\ell - 1}{p_\ell} = \frac{1}{2} \cdot 2^{\alpha_1} \prod_{\ell=2}^{r} p_\ell^{\alpha_\ell},$$

tai sievemmin muodossa

$$\prod_{\ell=2}^{r} p_\ell^{\alpha_\ell} \cdot \frac{p_\ell - 1}{p_\ell} = \prod_{\ell=2}^{r} p_\ell^{\alpha_\ell}.$$

Mutta koska jokainen tekijä $(p_\ell - 1)/p_\ell < 1$, on vasen puoli varmasti pienempi kuin oikea puoli, ja muita halutunlaisia lukuja, kuin luvun kaksi potenssit, ei ole.

17. Valitaan jotkin $2n$ eri alkulukua $p_1 < p_2 < p_3 < p_4 < \ldots < p_{2n-1} < p_{2n}$, mikä on varmasti mahdollista, sillä onhan alkulukuja äärettömän monta. Kiinalaisen jäännöslauseen nojalla on olemassa kokonaisluku x, jolle pätee

$$\begin{cases} x \equiv 0 \pmod{p_1 p_2}, \\ x \equiv -1 \pmod{p_3 p_4}, \\ x \equiv -2 \pmod{p_5 p_6}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv -(n-1) \pmod{p_{2n-1} p_{2n}}. \end{cases}$$

Nyt siis luvut x, $x+1$, $\ldots$, $x+(n-1)$ ovat n peräkkäistä kokonaislukua, joista x on jaollinen eri alkuluvuilla p_1 ja p_2, luku $x+1$ on jaollinen eri alkuluvuilla p_3 ja p_4, ja niin edelleen, ja väite on todistettu.

18. Lasketaan $1^2 \cdot 3^5 \cdot \ldots \cdot (p-2)^2$ modulo p. Täysin samanlaisella argumentilla voi myös selvittää, mitä on $2^2 \cdot 4^2 \cdot \ldots \cdot (p-1)^2$ modulo p. Wilsonin lauseen nojalla

$$\begin{aligned}
&1^2 \cdot 3^2 \cdot 5^2 \cdot \ldots \cdot (p-2)^2 \\
&\equiv 1 \cdot (p-2) \cdot 3 \cdot (p-4) \cdot 5 \cdot (p-6) \cdot \ldots \cdot (p-4) \cdot 3 \cdot (p-2) \cdot 1 \\
&\equiv 1 \cdot (-1) \cdot 2 \cdot 3 \cdot (-1) \cdot 4 \cdot 5 \cdot (-1) \cdot 6 \cdot \ldots \\
&\qquad \cdot (p-4) \cdot (-1) \cdot (p-3) \cdot (p-2) \cdot (-1) \cdot (p-1) \\
&\equiv (-1)^{(p-1)/2} \cdot (p-1)! \equiv (-1)^{(p-1)/2} \cdot (-1) \equiv (-1)^{(p+1)/2} \pmod{p}.
\end{aligned}$$

19. Wilsonin lauseen nojalla

$$\begin{aligned}
&\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv \left(\frac{p-1}{2}\right)! \left(\frac{p-1}{2}\right)! \\
&\equiv \left(\frac{p-1}{2}\right)! \cdot \frac{p-1}{2} \cdot \frac{p-3}{2} \cdot \ldots \cdot 3 \cdot 2 \cdot 1 \\
&\equiv \left(\frac{p-1}{2}\right)! \cdot (-1)\frac{p+1}{2} \cdot (-1)\frac{p+3}{2} \cdot \ldots \\
&\qquad \cdot (-1)\,(p-3) \cdot (-1)\,(p-2) \cdot (-1)\,(p-1) \\
&\equiv (p-1)! \cdot (-1)^{(p-1)/2} \equiv (-1) \cdot (-1)^{(p-1)/2} \equiv (-1)^{(p+1)/2} \pmod{p}.
\end{aligned}$$

Jos $p \equiv 1 \pmod 4$, niin $(p+1)/2$ on pariton, ja $(((p-1)/2)!)^2 \equiv -1 \pmod p$. Jos taas $p \equiv -1 \pmod 4$, niin $(p+1)/2$ on parillinen, ja $(((p-1)/2)!)^2 \equiv 1 \pmod p$, mistä seuraa myös, että $((p-1)/2)!$ on $\equiv 1$ tai $-1 \pmod p$.

20. Jos ei-negatiivisella kokonaisluvulla n on olemassa kokonaisluvut x, y ja z, joille

$$3^n = x^3 + y^3 + z^3,$$

niin varmasti

$$3^{n+3} = 3^3 \cdot 3^n = (3x)^3 + (3y)^3 + (3z)^3.$$

Riittää siis todistaa väite tapauksissa $n \in \{0, 1, 2\}$. Mutta nämä tapaukset ovat helppoja tarkistaa; onhan

$$1 = 1^3 + 0^3 + 0^3, \quad 3 = 1^3 + 1^3 + 1^3, \quad \text{ja} \quad 3^2 = 9 = 8 + 1 + 0 = 2^3 + 1^3 + 0^3.$$

21. Tarkastellaan yhtälöä modulo 13. Ensinnäkin, jos $n \in \mathbb{Z}$, niin $n^3 \equiv 0$, 1, 5, 8 tai 12 $\pmod{13}$. Lisäksi $n^4 \equiv 0$, 1, 3 tai 9 $\pmod{13}$. Suoraan yhteenlaskuja tekemällä todetaan, että annetussa yhtälössä vasen puoli voi olla vain

$$x^3 + y^4 \equiv 0, 1, 2, 3, 4, 5, 6, 8, 9, 10, 11 \text{ tai } 12 \pmod{13}.$$

Erityisesti $x^3 + y^4$ ei koskaan voi olla $\equiv 7 \pmod{13}$, eikä annetulla yhtälöllä siis voi olla kokonaislukuratkaisuita.

22. Oletetaan, että yhtälöllä on jokin positiivinen kokonaislukuratkaisu x, y, z. Koska x on positiivinen kokonaisluku, löytyy ratkaisu, jossa x on mahdollisimman pieni. Nyt siis tälle ratkaisulle pätee

$$x^3 + 3y^3 + 9z^3 - 3pxyz = 0.$$

Koska kaikki muut termit ovat kolmella jaollisia, on oltava $3 \mid x^3$, jolloin myös $3 \mid x$. Voidaan siis kirjoittaa $x = 3\xi$ jollakin $\xi \in \mathbb{Z}_+$. Sijoittamalla tämä takaisin yhtälöon saadaan

$$27\xi^3 + 3y^3 + 9z^3 - 9p\xi yz = 0.$$

Nyt kaikki muut termit ovat yhdeksällä jaollisia, joten $9 \mid 3y^3$, eli $3 \mid y^3$, ja edelleen $3 \mid y$. Nyt voidaan kirjoittaa $y = 3\eta$ jollakin $\eta \in \mathbb{Z}_+$. Sijoittamalla takaisin yhtälöön saadaan

$$27\xi^3 + 81\eta^2 + 9z^3 - 27p\xi\eta z = 0.$$

Koska kaikki muuta termit ovat 27 jaollisia, on $27 \mid 9z^3$, eli $3 \mid z^3$, ja edelleen $3 \mid z$. Voidaan siis kirjoittaa $z = 3\zeta$ jollakin $\zeta \in \mathbb{Z}_+$, ja sijoittamalla takaisin yhtälöön saadaan

$$27\xi^3 + 81\eta^3 + 243\zeta^3 - 81p\xi\eta\zeta = 0,$$

tai sievemmin

$$\xi^3 + 3\eta^3 + 9\zeta^3 - 3p\xi\eta\zeta = 0.$$

Mutta nyt ξ, η, ζ on myös positiivinen kokonaislukuratkaisu alkuperäiselle yhtälölle, ja $\xi < x$, vastoin ratkaisun x, y, z valintaa. Tämä ristiriita osoittaa, ettei alkuperäisellä yhtälöllä ole positiivisia kokonaislukuratkaisuita.

23. Oletetaan, että annetulla yhtälöllä olisi jokin positiivinen kokonaislukuratkaisu x, y, z. Todetaan aluksi, että jos x, y ja z olisivat kaikki parittomia, niin yhtälön vasen puoli olisi pariton, mutta oikea puoli parillinen. Siis ainakin yhden luvuista x, y ja z täytyy olla parillinen. Mutta nyt

$$x^2 + y^2 + z^2 \equiv 2xyz \equiv 0 \pmod 4,$$

ja koska jokainen neliö on $\equiv 0$ tai $1 \pmod 4$, on oltava $x \equiv y \equiv z \equiv 0 \pmod 2$. Merkitään $x = 2x_2$, $y = 2y_2$ ja $z = 2z_2$, missä $x_2, y_2, z_2 \in \mathbb{Z}_+$. Nyt x_2, y_2 ja z_2 toteuttavat yhtälön

$$x_2^2 + y_2^2 + z_2^2 - 4x_2y_2z_2 = 0.$$

Oletetaan seuraavaksi, että meillä on jollakin kokonaisluvulla $n \geqslant 2$ positiivinen kokonaislukuratkaisu x_n, y_n, z_n yhtälölle

$$x_n^2 + y_n^2 + z_n^2 - 2^n x_n y_n z_n = 0.$$

Tällöin

$$x_n^2 + y_n^2 + z_n^2 \equiv 0 \pmod 4,$$

eli jälleen voidaan kirjoittaa $x_n = 2x_{n+1}$, $y_n = 2y_{n+1}$ ja $z_n = 2z_{n+1}$ joillakin x_{n+1}, y_{n+1}, $z_{n+1} \in \mathbb{Z}_+$. Sijoittamalla lukujen x_n, y_n ja z_n toteuttamaan yhtälöön saadaan

$$x_{n+1}^2 + y_{n+1}^2 + z_{n+1}^2 - 2^{n+1} x_{n+1} y_{n+1} z_{n+1} = 0.$$

Tällä tavalla induktiolla saadaan jono x, x_2, x_3, ... positiivisia kokonaislukuja, joille $x > x_2 > x_3 > \ldots$, mikä on mahdotonta. Siis alkuperäisellä yhtälöllä ei voi olla positiivisia kokonaislukuratkaisuita.

24. Annetusta yhtälöstä seuraa, että

$$(x^3)^2 < x^6 + 3x^3 + 1 = y^4 = x^6 + 3x^3 + 1 < x^6 + 4x^3 + 4 = (x^3 + 2)^2,$$

eli on oltava $y^2 = x^3 + 1$. Mutta nyt annettu yhtälö muuttuu muotoon

$$x^6 + 3x^3 + 1 = x^6 + 2x^3 + 1,$$

mistä seuraa $x^3 = 0$, mikä on mahdotonta, koska luvun x piti olla positiivinen kokonaisluku. Siis positiivisia kokonaislukuratkaisuita ei ole.

25. Annetusta yhtälöstä seuraa, että

$$x^4 < x\,(x+1)\,(x+2)\,(x+3) = y^4,$$

ja että

$$y^4 = x^4 + 6x^3 + 11x^2 + 6x < x^4 + 8x^3 + 24x^2 + 32x + 16 = (x+2)^4.$$

On siis oltava $y = x + 1$. Mutta nyt annetusta yhtälöstä seuraakin, että

$$x^4 + 6x^3 + 11x^2 + 6x = x^4 + 4x^3 + 6x^2 + 4x + 1,$$

mikä sievenee muotoon

$$2x^3 + 5x^2 + 2x = 1.$$

Tämä viimeinen yhtälö ei voi päteä, koska x oli positiivinen kokonaisluku, ja siten $x \geqslant 1$ ja $2x^3 + 5x^2 + 2x \geqslant 2 + 5 + 2 > 1$.