Lösningar till tentamen i MMG100 Elementär talteori
2017-09-23 kl. 8.30–12.30

1. Bestäm resten av $2000 \cdot (2020^{2020} - 2 \cdot 2^{2020} - 2020^2)$ vid division med 2017. (2017 är ett primtal.)

Lösning: Vi har

$$\begin{aligned} 2000(2020^{2020} - 2 \cdot 2^{2020} - 2020^2) &\equiv -17(3^{2020} - 2 \cdot 2^{2020} - 3^2) \\ &\equiv -17(3^4 - 2 \cdot 2^4 - 3^2) \\ &= -17 \cdot 40 = -680 \equiv 1337 \bmod 2017. \end{aligned}$$

Då $0 \leq 1337 < 2017$ detta vara talets rest vid division med 2017, dvs resten är 1337.

2. Visa att ekvationen $x^2 + y^2 = 1003$ saknar heltalslösningar.

Lösning: Om vi betraktar ekvationen modulo 4 får vi $x^2 + y^2 \equiv 3 \bmod 4$, men denna har ingen lösning ty en heltalskvadrat är antingen kongruent med 0 eller 1 modulo 4, så de enda kongruensklasserna som är en summa av två kvadrater är $0 + 0 = 0$, $0 + 1 = 1$ och $1 + 1 = 2$. Det följer att den ursprungliga ekvationen saknar lösning.

3. Bestäm resten av 25! vid division med 29.

Lösning: Enligt Wilsons sats är $28! \equiv -1 \bmod 29$. Det följer att $-1 \equiv 25! \cdot 26 \cdot 27 \cdot 28 \equiv 25!(-3)(-2)(-1) = -6 \cdot 25! \bmod 29$, dvs $6 \cdot 25! \equiv 1 \bmod 29$, så 25! är en invers till 6 modulo 29. Genom att antingen använda Euklides utökade algoritm eller testa sig fram ser vi att 6 har 5 som invers modulo 29. Därmed är $5 \equiv 25! \bmod 29$. Då $0 \leq 5 < 29$ måste detta vara talets rest vid division med 29, dvs 25! har rest 5 vid division med 29.

4. Finn alla primitiva rötter modulo 19. Det är viktigt att du redovisar dina uträkningar.

Lösning: Vi börjar med att beräkna $2^1, 2^2, \ldots, 2^{18}$. För att spara plats skriver jag inte ut det här. Vi kan konstatera att $2^1, 2^2, \ldots 2^{17} \not\equiv 1$ men $2^{18} \equiv 1$ modulo 19, så $\mathrm{ord}_{19} 2 = 18 = \varphi(19)$. Vi ser att 2 är en primitiv rot modulo 19. De primitiva rötterna ges då av 2^i för alla i mellan 1 och 18 som är relativt prima $\varphi(19) = 18$. De primitiva rötterna är alltså $2^1 = 2, 2^5 \equiv 13, 2^7 \equiv 14, 2^{11} \equiv 15, 2^{13} \equiv 3, 2^{17} \equiv 10$ modulo 19.

5. Hur många inkongruenta heltalslösningar har ekvationen $x^6 \equiv 64 \bmod 105$? Du behöver inte beräkna lösningarna. (Tips: Dela upp i primalsfaktorer och använd Kinesiska restsatsen.)

Lösning: Då $105 = 3 \cdot 5 \cdot 7$ är ekvationen samma som

$$\begin{cases} x^6 \equiv 64 \equiv 1 \bmod 3 \\ x^6 \equiv 64 \equiv 4 \bmod 5 \\ x^6 \equiv 64 \equiv 1 \bmod 7. \end{cases}$$

Vi har $0^6 \equiv 0 \bmod 3$, $1^6 \equiv 1 \bmod 3$ och $2^6 = 64 \equiv 1 \bmod 3$, så första raden är uppfylld om $x \equiv 1$ eller $2 \bmod 3$.

På samma sätt, $0^6 \equiv 0 \bmod 5$, $1^6 \equiv 1 \bmod 5$, $2^6 = 64 \equiv 4 \bmod 5$, $3^6 \equiv (-2)^6 = 64 \equiv 4 \bmod 5$ och $4^6 \equiv (-1)^6 \equiv 1 \bmod 5$, så andra raden är uppfylld om $x \equiv 2$ eller $3 \bmod 5$.

Igen $0^6 \equiv 0 \bmod 7$, och enligt Fermats lilla sats har vi att om $x \not\equiv 0 \bmod 7$, så är $x^6 \equiv 1 \bmod 7$, så sista raden är uppfylld om $x \equiv 1, 2, 3, 4, 5$ eller $6 \bmod 7$.

Det följer att den ursprungliga ekvationen är uppfylld om

$$\begin{cases} x \equiv 1 \text{ eller } 2 \bmod 3 \\ x \equiv 2 \text{ eller } 3 \bmod 5 \\ x \equiv 1, 2, 3, 4, 5 \text{ eller } 6 \bmod 7. \end{cases}$$

Enligt Kinesiska restsatsen motsvarar varje kombination av högerled en unik lösning x modulo 105, så totalt får vi $2 \cdot 2 \cdot 6 = 24$ inkongruenta lösningar.

6. Två positiva heltal a och b uppfyller att deras största gemensamma delare (a, b) och deras minsta gemensamma multipel $[a, b]$ båda är kvadrater. Visa att a och b själva då måste vara kvadrater.

Lösning: Låt $p_1, p_2, \ldots p_n$ beteckna de primtal som delar minst en av a och b. Skriv $a = p_1^{a_1} \cdot \cdots \cdot p_n^{a_n}$ och $b = p_1^{b_1} \cdot \cdots \cdot p_n^{b_n}$. Då är

$$(a, b) = p_1^{\min(a_1, b_1)} \cdot \cdots \cdot p_n^{\min(a_n, b_n)}$$

och

$$[a, b] = p_1^{\max(a_1, b_1)} \cdot \cdots \cdot p_n^{\max(a_n, b_n)}.$$

Eftersom (a, b) och $[a, b]$ är kvadrater är $\min(a_i, b_i)$ och $\max(a_i, b_i)$ jämna för alla $1 \leq i \leq n$. Detta innebär att a_i och b_i måste vara jämna för alla $1 \leq i \leq n$, dvs a och b är kvadrater.

7. Låt p vara ett udda primtal sådant att $p \equiv 1 \bmod 8$. Visa att $\frac{p-1}{2}$ är en kvadratisk rest modulo p.

Lösning: Vi noterar att $2 \cdot \frac{p-1}{2} = p - 1 \equiv -1 \bmod p$. Därmed är $\left(\frac{2}{p}\right)\left(\frac{(p-1)/2}{p}\right) = \left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right)$. Då $p \equiv 1 \bmod 8$ och därmed även $p \equiv 1 \bmod 4$ är $\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right) = 1$, så $1 \cdot \left(\frac{(p-1)/2}{p}\right) = 1$ och $\frac{p-1}{2}$ är en kvadratisk rest modulo p.

8(a): Beräkna den största gemensamma delaren mellan $10^8 - 1 = 99999999$ och $10^{13} - 1 = 9999999999999$.

Lösning: Euklides algoritm ger

$$\begin{aligned} 9999999999999 &= 99999999 \cdot 100000 + 99999 \\ 99999999 &= 99999 \cdot 1000 + 999 \\ 99999 &= 999 \cdot 100 + 99 \\ 999 &= 99 \cdot 10 + 9 \\ 99 &= 9 \cdot 11 + 0. \end{aligned}$$

Vi ser att den största gemensamma delaren är 9.

8(b): Låt a och b vara positiva heltal. Bevisa en allmän formel för $(10^a - 1, 10^b - 1)$.

Lösning: Från uträkningen i (a) ser det ut som att om man gör Euklides algoritm på tal som bara består av nior, så kommer alla rester man får också bara bestå av nior.

Låt oss börja med att betrakta heltalsdivision mellan två tal som bara består av 9:or. För enkelhets skull, säg talet bestående av a stycken nior och det bestående av b stycken nior (dvs $10^a - 1$ och $10^b - 1$). Skriv $a = bq + r$ där $0 \leq r < b$. Vi kan dela upp siffrorna i $10^a - 1$ i q grupper av b stycken nior vardera och en sista grupp av r stycken nior. Detta ger

$$\begin{aligned} 10^a - 1 &= \underbrace{999999999999999999999999}_{a \text{ st}} \\ &= \underbrace{\underbrace{999999999999999999999999}_{b \text{ st}} \underbrace{}_{b \text{ st}} \underbrace{}_{b \text{ st}} \underbrace{}_{b \text{ st}}}_{q \text{ grupper}} \underbrace{999}_{r \text{ st}} \\ &= \underbrace{\underbrace{000001000001000001000001}_{b \text{ siffror}} \underbrace{}_{b \text{ siffror}} \underbrace{}_{b \text{ siffror}} \underbrace{}_{b \text{ siffror}}}_{q \text{ grupper}} \underbrace{000}_{r \text{ st}} \cdot \underbrace{999999}_{b \text{ st}} + \underbrace{999}_{r \text{ st}} \end{aligned}$$

Då $0 \leq$ talet bestående av r stycken nior $<$ talet bestående av b stycken nior, måste talet bestående av r nior vara resten vid divisionen. Vi drar slutsatsen att om a har rest r vid division med b så har a stycken nior r stycken nior som rest vid division med b stycken nior.

Från detta följer att om vi utför Euklides algoritm på $10^a - 1$ och $10^b - 1$ kommer antalet nior vi får som rest i varje steg motsvara resterna vi får om vi utför Euklides algoritm på a och b. Därmed är sista nollskilda resten, och därmed den största gemensamma delaren, talet bestående av (a, b) stycken nior. Det vill säga $(10^a - 1, 10^b - 1) = 10^{(a,b)} - 1$.