

Vilket svar är rätt?

R: röd, G: grön, B: blå

1. Vilken/vilka av följande är $\equiv_{10} 267^{10}$?

R: 1, G: 19, B: 67

2. Vilken/vilka av följande är $\equiv_{107} 1077^{213}$?

R: 1, G: 14, B: 114

3. Finns det något $x \in \mathbb{Z}_{13}$ med $x^2 + 1 = 0$?

R: Ja, G: Kanske, B: Nej

4. $x = 25$ uppfyller $x \equiv_7 4$, $x \equiv_{11} 3$.

Hur många x med $0 \leq x \leq 1000$ gör det?

R: 11, G: 12, B: 13

5. $x \in \mathbb{Z}_{77}$ beskrivs av $([x]_7, [x]_{11})$.

Vilket/vilka av följande är inverterbart/a?

R: (2, 10), G: (0, 7), B: (1, 0)

6. Vad är $\phi(77)$ (antalet inverterbara element i $\mathbb{Z}_{77}$)?

R: 55, G: 60, B: 66

Svar:

1. G, ty $267^{10} \equiv_{10} 7^{10} = (7^4)^2 \cdot 7^2 \equiv_{10} 1^2 \cdot 49 \equiv_{10} 9 \equiv_{10} 19$,
enligt Eulers sats (eftersom $\phi(10) = |\{1, 3, 7, 9\}| = 4$ och $\text{sgd}(7, 10) = 1$).
2. B, ty 107 är primtal och $107 \nmid 1077$, så enligt Fermats lilla sats är
 $1077^{213} = (1077^{106})^2 \cdot 1077 \equiv_{107} 1^2 \cdot 1077 \equiv_{107} 7 \equiv_{107} 114$.
3. R, ty $5^2 + 1 = 26 \equiv_{13} 0$.
(I själva verket finns $x \in \mathbb{Z}_p$, p primtal, med $x^2 + 1 = 0$ omm $p = 2$ eller $p \equiv_4 1$.)
4. B, ty $\text{sgd}(7, 11) = 1$ och enligt kinesiska restsatsen är
 $x \equiv_7 4$, $x \equiv_{11} 3$ omm $x \equiv_{7 \cdot 11} 25$, dvs omm $x = 25 + 77n$, $n \in \mathbb{Z}$.
 $0 \leq 25 + 77n \leq 1000$ precis för $n = 0, 1, \dots, 12$ ($77 \cdot 13 = 1001$).
5. R, ty $(a, b) \in \mathbb{Z}_7 \times \mathbb{Z}_{11}$ är inverterbart omm a, b är inverterbara i $\mathbb{Z}_7, \mathbb{Z}_{11}$.
($(a, b)^{-1} = (a^{-1}, b^{-1})$, ty $(1, 1)$ svarar mot $1 \in \mathbb{Z}_{77}$.)
6. G, ty enligt 5. beskrivs de inverterbara precis av de (a, b) som har a, b inverterbara (i $\mathbb{Z}_7, \mathbb{Z}_{11}$). 6 olika a , 10 olika b ger $6 \cdot 10$ olika (a, b) .