MIDTERM SAMPLE

SOLUTIONS

2021-10-21

1. X Euclidean gcd $\qquad d = 29 \cdot s + 12 t$

a) $a = 29 \qquad b = 12$

d	s	t
29	1	0
12	0	1
$29 - 2 \cdot 12 = 5$	$1 - 2 \cdot 0 = 1$	$0 - 2 \cdot 1 = -2$
$12 - 2 \cdot 5 = 2$	$0 - 2 \cdot 1 = -2$	$1 - 2(-2) = +5$
RETURN → $5 - 2 \cdot 2 = 1$	$1 - 2 \cdot (-2) = +5$	$-2 - 2 \cdot +5 = -12$
$2 - 2 \cdot 1 = 0$		

$1 = 145 + -144$

$d = 29 \cdot s + 12 \cdot t$

$d = 1 \qquad s = 5 \qquad t = -12$

b) 110, 28

	d	s	t
	110	1	0
	28	0	1
	$110 - 3 \cdot 28 = 26$	$1 - 3 \cdot 0 = 1$	$0 - 3 \cdot 1 = -3$
RETURN →	$28 - 1 \cdot 26 = 2$	$0 - 1 \cdot 1 = -1$	$1 - 1 \cdot -3 = 4$
	$26 - 13 \cdot 2 = 0$		
	$d = 2$	$s = -1$	$t = 4$

$$2 = -1 \cdot 110 + 4 \cdot 28 \quad ✓$$

c) 55, 34

d	s	t
55	1	0
34	0	1
$55 - 1 \cdot 34 = 21$	$1 - 1 \cdot 0 = 1$	$0 - 1 \cdot 1 = -1$
$34 - 1 \cdot 21 = 13$	$0 - 1 \cdot 1 = -1$	$1 - 1 \cdot (-1) = 2$
$21 - 1 \cdot 13 = 8$	$1 - 1 \cdot (-1) = 2$	$-1 - 1 \cdot 2 = -3$
$13 - 1 \cdot 8 = 5$	$(-1) - 1 \cdot 2 = -3$	$2 - 1 \cdot (-3) = 5$
$8 - 1 \cdot 5 = 3$	$2 - 1 \cdot (-3) = 5$	$-3 - 1 \cdot 5 = -8$
$5 - 1 \cdot 3 = 2$	$(-3) - 1 \cdot 5 = -8$	$5 - 1 \cdot (-8) = 13$

$3-1\cdot 2=1$	$5-1\cdot(-8)=13$	$-8-1\cdot 13=-21$
$2-2\cdot 1=0$		

$d=1, \quad s=13, \quad t=-21$

$1=55\cdot 13+34\cdot(-21)$ ✓

1A: $1=29\cdot 5+12\cdot(-12)$

1B: $2=110\cdot(-1)+28\cdot(+4)$

1C: $1=55\cdot 13+34\cdot(-21)$

2A: $29x + 12y = 300$

WE KNOW ALREADY:

$$29 \cdot 5 + 12 \cdot (-12) = 1 \qquad (1.A)$$

CHECK: $\gcd(29, 12)$ divides 300 $\xrightarrow{\text{YES}}$ WE HAVE SOLS. ✓

$\times 300$

$$29 \cdot (\underbrace{1500}_{x_0}) + 12 \cdot (\underbrace{-3600}_{y_0}) = 300$$

BASIC SOL:

$x_0 = 1500 \qquad y_0 = -3600$

INFINITELY MANY:

$\forall k \in \mathbb{Z}$: $x_k = x_0 + 12k$

$y_k = y_0 - 29k$

$x_k > 0 \qquad 1500 + 12k > 0 \rightarrow k > -125$

$y_k > 0 \qquad -3600 - 29k > 0 \rightarrow k < -124.13\ldots$

$k \leq -125$ ↯

NO SOL.

2B:

$28x \equiv 33 \quad (110)$

1B: $2 = 110 \cdot (-1) + 28 \cdot (+4)$ ←

CHECK: 2 divides 33

NO ↙

NO SOLS

✓

READY

YES ↘ (E.g. 6 ✓) $\quad 28x \equiv 6 \ (110)$

$28 \cdot 4 = 2 - 110 \cdot (-1)$ ←

⇓

$28 \cdot 4 \equiv 2 \quad (110) \quad /\times 3$

$28 \cdot 12 \equiv 6 \quad (110)$

2G

$$\begin{cases} x \equiv \overset{a_1}{7} \ (\overset{m_1}{55}) \\ x \equiv \overset{a_2}{5} \ (\overset{m_2}{34}) \end{cases} \overset{\text{C.R.T}}{\Longleftrightarrow} x \equiv \underset{A}{?} \ (55 \cdot 34)$$

$$1 = 55 \cdot \underset{s}{13} + 34 \cdot \underset{t}{(-21)}$$

FORMULA:

$$\text{GCD}(m_1, m_2) = 1 \quad \begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \end{cases} \Longleftrightarrow x \equiv A \ (m_1 \cdot m_2)$$

$$\downarrow$$

$$\text{GCD} = 1 = m_1 \cdot s + m_2 \cdot t$$

$$A = m_1 \cdot s \cdot a_2 + m_2 \cdot t \cdot a_1$$

$$= 55 \cdot 13 \cdot 5 + 34 \cdot (-21) \cdot 7$$

$$= -1423 \equiv 447 \ (55 \cdot 34)$$

$$\equiv 447 \ (1870)$$

4. $2023^{(2025^{2027})} \bmod 100$ $\quad$ (B: 37 C: 1001)

EULER'S THEOREM:

$$\forall m, a;\ \gcd(m,a)=1 \Rightarrow a^{\varphi(m)} \equiv 1 \ (m)$$

$$\xRightarrow[\text{COR.}]{} \quad a^{N} \bmod m = a^{N-\varphi(m)} \bmod m = a^{(N \% \varphi(m))} \bmod m$$

E.g.: $\varphi(100) = 40$ $\quad$ SAGE: euler_phi

$$91^{1320738} \bmod 100$$

$$\parallel$$

$$91^{(\ldots\ldots \% 40)} \equiv 91^{18} \ (100)$$

4A :

$$2023^{\left(2025^{2027}\right)} \mod 100 \qquad \varphi(100) = 40$$

SUBPROBLEM:

$$2025^{2027} \equiv ? \quad (40)$$

$$\varphi(40) = 16$$

$$2025^{(2027 \% 16)} \equiv 2025^{11} \quad (40)$$

$$\equiv 25^{11} \quad (40)$$

$$\equiv 25$$

$$2023^{25} \mod 100 = 23^{25} \mod 100 = 43$$