Outline of solutions

1.a) $\gcd(14,29)=1 \Rightarrow 14x=1$ has a solution in $\mathbb{Z}/29\mathbb{Z}$.

ad hoc method:

$$2\times 14x = 2 \Rightarrow -x = 2$$

$$\Rightarrow x = -2 = 27.$$

b) $\gcd(7,18)=1 \Rightarrow 7x=4$ has a solution in $\mathbb{Z}/18\mathbb{Z}$.

(Euclid Algorithm)

$$18 = 7\times 2+4 \Rightarrow 4 = -7\times 2+18$$

$$7 = 4\times 1+3 \Rightarrow 3 = -4\times 1+7$$

$$4 = 3\times 1+1 \Rightarrow 1 = -3\times 1+4$$

$$\Rightarrow 1 = -3\times 1+4$$

$$= -(-4\times 1+7)+4 = 4\times 2-7\times 1$$

$$= (-7\times 2+18)\times 2 - 7\times 1$$

$$= \underline{-7\times 5}+18\times 2$$

$$7x=4 \Rightarrow -5\times 7x = -5\times 4$$

$$\Rightarrow \quad x = -20 = 16$$

c) $\gcd(14,36) = 2 \mid 8 \Rightarrow 14x = 8$ has a solution in $\mathbb{Z}/36\mathbb{Z}$.

$$14x \overset{36}{\equiv} 8 \iff 7x \overset{18}{\equiv} 4$$

$$\iff x \overset{18}{\equiv} 16 \quad (\text{part } \underline{\underline{b}})$$

$$\iff x = 16 \text{ or } 34 \text{ in } \mathbb{Z}/36\mathbb{Z}.$$

d) $\gcd(14,36) = 2 \nmid 1 \Rightarrow 14x = 1$ has no solution in $\mathbb{Z}/36\mathbb{Z}$.

2. Find $\min\{|x|+|y| \mid x,y \in \mathbb{Z},\ 53x+29y=3\}$.

<u>First</u> Check if it has a solution.

$$\gcd(29,53) = 1 \mid 3. \checkmark$$

<u>Second</u> Use Euclid Algorithm to find a solution.

$$53 = 29 \times 1 + 24 \Rightarrow 24 = -29 \times 1 + 53$$

$$29 = 24 \times 1 + 5 \Rightarrow 5 = -24 \times 1 + 29$$

$$24 = 5 \times 4 + 4 \Rightarrow 4 = -5 \times 4 + 24$$

$$5 = 4 \times 1 + 1 \Rightarrow 1 = -4 \times 1 + 5$$

$$1 = -4 \times 1 + 5$$
$$= -(-5 \times 4 + 24) + 5 = 5 \times 5 - 24$$
$$= (-24 \times 1 + 29) \times 5 - 24 = -24 \times 6 + 29 \times 5$$
$$= -(-29 \times 1 + 53) \times 6 + 29 \times 5$$
$$= 29 \times 11 - 53 \times 6$$

$\Rightarrow$ $x_0 = -6 \times 3 = -18$ and $y_0 = 11 \times 3 = 33$
is a solution of $53x + 29y = 3$.

<u>Third</u> Find all the solutions.

$$\begin{cases} x = x_0 + 29t \\ y = y_0 - 53t \end{cases} \quad \text{for any } t \in \mathbb{Z}.$$

<u>Forth</u> Find the min:

$$|x| = |-18 + 29t| = \begin{cases} 29t - 18 & t \geq 1 \\ 18 - 29t & t \leq 0 \end{cases}$$

$$|y| = |33 - 53t| = \begin{cases} 53t - 33 & t \geq 1 \\ 33 - 53t & t \leq 0 \end{cases}$$

$$\Rightarrow |x|+|y| = \begin{cases} 82t - 51, & t \geq 1 \\ 51 - 82t, & t \leq 0 \end{cases}$$

If $t \geq 1$, the min $= 82 - 51 = 31$

If $t \leq 0$, the min $= 51$

So $\min |x|+|y| = 31$ and the equality holds iff $x = 11$ and $y = -20$.

- Prove $\gcd(2^{2^n}+1, 2^{2^m}+1) = 1$ if $n \neq m$.

<u>Proof</u>. Without loss of generality we will assume

$$m < n.$$

Let $d = \gcd(2^{2^m}+1, 2^{2^n}+1)$. Thus

$$2^{2^m} \equiv -1 \pmod d \wedge 2^{2^n} \equiv -1 \pmod d.$$

On the other hand, $2^{2^n} = 2^{2^{n-m+m}} = 2^{2^{n-m} \cdot 2^m}$

$$= \left(2^{2^m}\right)^{2^{n-m}} \overset{d}{\equiv} (-1)^{2^{n-m}} = 1$$

Therefore $1 \overset{d}{\equiv} -1$, i.e. $d \mid 2$. Since $d \mid 2^{2^m}+1$, d is odd. Hence $d = 1$. ∎

a) $x^2 = 1$ in $\mathbb{Z}/p\mathbb{Z} \iff x^2 \overset{p}{\equiv} 1$

$\iff p \mid x^2 - 1 = (x-1)(x+1)$

$\iff p \mid x-1 \lor x+1$

$\iff x \overset{p}{\equiv} 1 \lor x \overset{p}{\equiv} -1.$

$\iff x = \pm 1$ in $\mathbb{Z}/p\mathbb{Z}$.

b) $\forall a \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, $\gcd(a,p) = 1 \Rightarrow$

$\exists x, y \in \mathbb{Z}$, $ax + py = 1 \Rightarrow$

$\exists x \in \mathbb{Z}$, $ax \equiv 1 \pmod{p} \Rightarrow$

$\exists a' \in \mathbb{Z}/p\mathbb{Z}$, $aa' = 1$.

(This question is equivalent to say

$$U(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}.)$$

Moreover if $aa'_1 = 1 = aa'_2$, then

$$a'_1 = a'_1 \cdot 1 = a'_1 \cdot (aa'_2) = (a'_1 a) a'_2 = 1 \cdot a'_2 = a'_2.$$

So such a' is unique.

c) From ⓐ and ⓑ, we conclude that

any $a \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ has a unique inverse

a^{-1} and $a^{-1}=a$ iff $a=\pm 1$.

Thus $1\cdot 2\cdot 3\cdot\dots\cdot(p-1)\overset{p}{\equiv} 1\cdot(p-1)\overset{p}{\equiv} -1$.

Prove $7 \nmid 2^n+1$ for any non-negative integer n.

Pf. $2^0 \overset{7}{\equiv} 1$, $2^1 \overset{7}{\equiv} 2$, $2^2 \overset{7}{\equiv} 4$, $2^3 \overset{7}{\equiv} 1$.

Thus, for any $k\in\mathbb{N}\cup\{0\}$, we have

$$2^{3k} \overset{7}{\equiv} (2^3)^k \overset{7}{\equiv} 1.$$

$$2^{3k+1} \overset{7}{\equiv} (2^3)^k\cdot 2 \equiv 2$$

$$2^{3k+2} \overset{7}{\equiv} (2^3)^k\cdot 4 \equiv 4.$$

Hence $2^{3k}+1\equiv 2$, $2^{3k+1}+1\equiv 3$ & $2^{3k+2}+1\equiv 5$.

Prove $\gcd(2^n-1, 2^m-1) = 2^{\gcd(n,m)}-1$.

Pf. Let $a_0=n$, $a_1=m$ and define a_i's using Euclid Algorithm, i.e.

$$a_0 = a_1\cdot q_0 + a_2 \qquad 0\le a_2 < a_1.$$

$$a_1 = a_2\cdot q_1 + a_3 \qquad 0\le a_3 < a_2.$$

$$\vdots$$

$$a_{i-1} = a_i \cdot q_{i-1} + a_{i+1} \qquad 0 \le a_{i+1} < a_i .$$

$$\vdots$$

$$a_{k-1} = a_k \cdot q_{k-1} + a_{k+1} \qquad 0 \le a_{k+1} < a_k$$

$$a_k = a_{k+1} \cdot q_k .$$

By Euclid Algorithm we know that

$$a_{k+1} = \gcd(m,n)$$

Now, by strong induction, we prove that for any i

$$2^{a_i} \equiv 1 \pmod{d},$$

where $d = \gcd(2^n - 1, 2^m - 1)$.

<u>Base cases</u>: Since $d \mid 2^n - 1$ & $d \mid 2^m - 1$, we have $2^{a_0} \equiv 2^{a_1} \equiv 1 \pmod{d}$.

<u>Induction Step</u>:

We prove $2^{a_{i-1}} \equiv 1 \wedge 2^{a_i} \equiv 1 \Rightarrow 2^{a_{i+1}} \equiv 1$.

By the above equalities we have

$$1 \equiv 2^{a_{i-1}} = 2^{a_i q_{i-1} + a_{i+1}} = \left(2^{a_i}\right)^{q_{i-1}} \cdot 2^{a_{i+1}}$$

$$\equiv (1)^{q_{i-1}} \cdot 2^{a_{i+1}} \equiv 2^{a_{i+1}} .$$

So this proves that $d \mid 2^{\gcd(m,n)} - 1$. I

On the other hand,

$$2^n = \left(2^{\gcd(m,n)}\right)^{n/\gcd(m,n)} \overset{2^{\gcd(m,n)}-1}{\equiv} 1.$$

$$2^m = \left(2^{\gcd(m,n)}\right)^{m/\gcd(m,n)} \overset{2^{\gcd(m,n)}-1}{\equiv} 1.$$

Hence $2^{\gcd(m,n)} - 1$ is a common divisor of $2^n - 1$ and $2^m - 1$. Therefore

$$2^{\gcd(m,n)} - 1 \leq d. \quad \text{II}$$

I, II $\Rightarrow d = 2^{\gcd(m,n)} - 1$. ∎