

C1

H.W. #3: Number Theory

§4.4: (1) a) b), (6) §5.2: 3; (5); §5.3: (4) 10; §5.4: 2, 3

§4.4 #1a) $\gcd(25, 29) = 1$; Hence $25x \equiv 15 \pmod{29}$

has a unique solution modulo 29.

$$\begin{array}{r} 1 \\ 25 \overline{) 29} \\ \underline{25} \\ 4 \end{array} \quad \begin{array}{r} 6 \\ 4 \overline{) 25} \\ \underline{24} \\ 1 \end{array} \quad \begin{aligned} 1 &= 25 - 4 \times 6 \\ &= 25 - (29 - 25) \times 6 \\ &= (-6) \times 29 + 7 \times 25 \end{aligned}$$

Hence $15 = (-15 \times 6) \times 29 + (15 \times 7) \times 25$

Thus $25x \equiv 15 \pmod{29}$

Therefore the solution is $x = 105 + 29t$, $t \in \mathbb{Z}$

(or $x = 18 + 29t$, $t \in \mathbb{Z}$)

#1b) We use a different method.

$$5x \equiv 2 \pmod{26}$$

Multiplying both sides by 5:

$$25x \equiv 10 \pmod{26}$$

$$-1 \cdot x \equiv 10 \pmod{26}$$

$$x \equiv -10 \pmod{26} \equiv 16 \pmod{26}$$

Hence solution is $x = 16 + 26t$, $t \in \mathbb{Z}$

§4.4 #6

$$\begin{aligned} a &\equiv 0 \pmod{2} & (1) \\ a &\equiv -1 \pmod{3} & (2) \\ a &\equiv -2 \pmod{4} & (3) \\ a &\equiv -3 \pmod{5} & (4) \\ a &\equiv -4 \pmod{6} & (5) \end{aligned}$$

(2)

From (1), we have $a = 2k$.

plugging into (2): $2k \equiv -1 \pmod{3}$

$$\Rightarrow (-1)k \equiv -1 \pmod{3} \Rightarrow k \equiv 1 \pmod{3}$$

Hence $k = 1 + 3p$, and $a = 2k = 2(1 + 3p) = 2 + 6p$.

plug this into (3):

$$2 + 6p \equiv -2 \pmod{4} \Rightarrow 6p \equiv -4 \pmod{4}$$

$$\Rightarrow 2p \equiv -4 \pmod{4} \Rightarrow p \equiv -2 \pmod{2} \equiv 0 \pmod{2}$$

Hence $p = 2s$, and $a = 2 + 6p = 2 + 12s$.

plug this into (4):

$$2 + 12s \equiv -3 \pmod{5}$$

$$12s \equiv -5 \pmod{5} \Rightarrow 2s \equiv -0 \pmod{5}$$

$$\Rightarrow 6s \equiv -0 \pmod{5} \Rightarrow s \equiv 0 \pmod{5}$$

Hence $s = 5t$, and $a = 2 + 12s = 2 + 60t$.

plugging this into (5):

$$2 + 60t \equiv -4 \pmod{6}$$

$$\Rightarrow 60t \equiv -6 \pmod{6} \equiv 0 \pmod{6}$$

Hence t can be any integer.

Therefore the general solution is $a = 2 + 60t, t \in \mathbb{Z}$,
and the smallest solution > 2 is 62.

(23)

§5.2 #3 $13 \mid 11^{12n+6} + 1 \iff 11^{12n+6} \equiv -1 \pmod{13}.$

By Fermat's Thm:

$$11^{12} \equiv 1 \pmod{13}.$$

Hence $11^{12n} \equiv 1^n \pmod{13} \equiv 1 \pmod{13}. \quad (1)$

Also, $11^2 \equiv 121 \equiv 4 \pmod{13}$

$$\implies (11^2)^3 \equiv 64 \pmod{13} \equiv -1 \pmod{13} \quad (2)$$

Multiplying (1) and (2): $11^{12n+6} \equiv -1 \pmod{13}.$

§5.2 #5

$$60 \mid a^4 + 59 \iff a^4 \equiv -59 \equiv 1 \pmod{60}$$

$$60 = 2^2 \cdot 3 \cdot 5.$$

It suffices to prove that

$$a^4 \equiv 1 \pmod{3} \quad (1)$$

$$a^4 \equiv 1 \pmod{5} \quad (2)$$

$$a^4 \equiv 1 \pmod{2^2} \quad (3)$$

Since $\gcd(30, a) = 1$, $3 \nmid a$. By Fermat's Thm,

$$a^2 \equiv 1 \pmod{3} \implies a^4 \equiv 1 \pmod{3}. \quad (1)$$

$$5 \nmid a \implies a^4 \equiv 1 \pmod{5}. \quad (2)$$

$$2 \nmid a \implies a = 2k+1 \text{ for some } k \in \mathbb{Z}.$$

$$\text{Hence } a^2 = 4(k^2 + k) + 1 \equiv 1 \pmod{2^2}$$

$$\implies a^4 \equiv 1 \pmod{2^2}. \quad (3)$$

(4)

5.3 (#4) By Wilson's Thm,

$$18! \equiv -1 \pmod{19} \quad (1)$$

$$\& \quad 22! \equiv -1 \pmod{23} \quad (2)$$

(Note that $437 = 19 \cdot 23$.)

Since $19 \cdot 20 \cdot 21 \cdot 22 \equiv (-4)(-3)(-2)(-1) \equiv 24 \equiv 1 \pmod{23}$,
from (2), we have

$$18! \equiv -1 \pmod{23} \quad (3)$$

Since $\gcd(19, 23) = 1$, from (1) & (3) we have

$$18! \equiv -1 \pmod{19 \cdot 23} \equiv -1 \pmod{437}.$$

#10 (a) By Wilson's Thm, we have

$$(p-1)! \equiv -1 \pmod{p}.$$

$$\text{Since } p = 4k+3, \quad (p-1)! = (4k+2)! = 1 \cdot 2 \cdots (2k+1) \cdot (2k+2) \cdot (2k+3) \cdots (4k+2).$$

$$\text{Since } 4k+2 \equiv -1 \pmod{p}$$

...

$$2k+3 \equiv -(2k) \pmod{p}$$

$$2k+2 \equiv -(2k+1) \pmod{p}$$

$$\Rightarrow (2k+2)(2k+3) \cdots (4k+2) \equiv (-1)^{2k+1} 1 \cdots (2k)(2k+1) \pmod{p}.$$

$$\text{Hence } (p-1)! \equiv -[(2k+1)!]^2 \equiv -1 \pmod{p}.$$

(L5)

Therefore, $[(-2k+1)!]^2 = \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv 1 \pmod{p}$.

Hence $\left(\frac{p-1}{2}\right)! \equiv 1 \pmod{p}$ or $\left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p}$.

554 #2 Since $(x+50)^2 \equiv x^2 + 100(-x+25) \equiv x^2 \pmod{100}$,

and $(50-x)^2 \equiv x^2 - 100(-x-25) \equiv x^2 \pmod{100}$

As x runs from 0 to 25,

$50-x$ takes values from 25 to 50

and as x runs from 0 to 50,

$50+x$ takes values from 50 to 100.

Therefore, it suffices to find $k^2 \pmod{100}$, $0 \leq k \leq 25$.

Modulus 100, we have

$$0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 16,$$

$$5^2 \equiv 25, 6^2 \equiv 36, 7^2 \equiv 49, 8^2 \equiv 64, 9^2 \equiv 81$$

$$10^2 \equiv 0, 11^2 \equiv 21, 12^2 \equiv 44, 13^2 \equiv 69, 14^2 \equiv 96$$

$$15^2 \equiv 25, 16^2 \equiv 56, 17^2 \equiv 89, 18^2 \equiv 24, 19^2 \equiv 61$$

$$20^2 \equiv 0, 21^2 \equiv 41, 22^2 \equiv 84, 23^2 \equiv 29, 24^2 \equiv 76$$

$$25^2 \equiv 25.$$

Listed in increasing order, we have:

00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56,
61, 64, 69, 76, 81, 84, 89, 96.

(C6)

85.5

#3

$2^{11} - 1 = 2047$. The least integer $\geq \sqrt{2047}$ is 46.

$$46^2 - 2047 = 69 \quad \times$$

$$47^2 - 2047 = 162 \quad \times$$

$$48^2 - 2047 = 257 \quad \times$$

$$49^2 - 2047 = 354 \quad \times$$

$$50^2 - 2047 = 453 \quad \times$$

$$51^2 - 2047 = 554 \quad \times$$

$$52^2 - 2047 = 657 \quad \times$$

$$53^2 - 2047 = 762 \quad \times$$

$$54^2 - 2047 = 869 \quad \times$$

$$55^2 - 2047 = 978 \quad \times$$

$$56^2 - 2047 = 1089 = 33^2$$

Hence $2047 = 56^2 - 33^2$

$$= (56 + 33)(56 - 33)$$

$$= 89 \cdot 23$$

□