Pure Mathematics 3370
Solutions to Selected Problems in the Course Manual

Chapter 1

1.(a) When $n = 1$, $16^1 = 16$ clearly ends in 6. Assume that 16^k ends in 6. That is, $16^k = 10a + 6$ for some positive integer a. Then

$$16^{k+1} \;=\; 16^k \cdot 16 \;=\; (10a+6)16 \;=\; 160a + 96 \;=\; 10(16a+9)+6.$$

Hence 16^{k+1} ends in 6 and so for all integers $n \geq 1$, 16^n ends in 6.

3. For $n = 1$, $(2n)! = 2! = 2$ and $2^{2n}(n!)^2 = 2^2(1!)^2 = 4$. Since $2 < 4$, the result holds for $n = 1$. Assume $(2k)! < 2^{2n}(k!)$, then

$$\begin{aligned} (2(k+1))! = (2k+2)! &= (2k+2)(2k+1)(2k)! \\ &< (2k+2)(2k+2)(2k)! = 2^2(k+1)^2(2k)! \\ &< 2^2(k+1)^2 2^{2k}(k!)^2 = 2^{2(k+1)}((k+1)!)^2. \end{aligned}$$

Hence, the inequality holds when k is replaced by $k+1$. Hence for all positive integers n, $(2n)! < 2^{2n}(n!)^2$.

11.(d) For $n = 1$, $n^3 - n = 1 - 1 = 0$ and 0 is divvisible by 6. Assume $k^3 - k = 6a$ for some integers a. Then

$$\begin{aligned} (k+1)^3 - (k+1) &= k^3 + 3k^2 + 3k + 1 - (k+1) \\ &= k^3 - k + 3k(k+1) \\ &= 6a + 3k(k+1). \end{aligned}$$

But $k(k+1)$ is the product of two consecutive integers, and so must be a multiple of 2. Hence $(k+1)^3 - (k+1) = 6a + 3(2b)$ for some integer b, and so $(k+1)^3 - (k+1)$ is divvisible by 6. Hence, in general, $6 \mid (n^2 - n)$.

(h) For $n = 0$, $11^{0+2} + 12^{2(0)+1} = 121 + 12 = 133$. Assume $11^{k+2} + 12^{2k+1} = 133a$ for some $a \in \mathbb{Z}$, then

$$\begin{aligned} 11^{k+3} + 12^{2k+3} &= 11 \cdot 11^{k+2} + 12^2 \cdot 12^{2k+1} \\ &= 11 \cdot 11^{k+2} + (133+11)12^{2k+1} \\ &= 11(11^{k+2} + 12^{2k+1}) + 133 \cdot 12^{2k+1} \\ &= 11(133a) + 133 \cdot 12^{2k+1}. \end{aligned}$$

Clearly the last number is divvisible by 133. Hence $133 \mid (11^{n+2} + 12^{2n+1})$ for all $n \geq 0$.

16.(d) For $n = 2$, $\alpha^2 = 1 + \alpha = F_1 + \alpha F_2$ and hence $\alpha^n = F_{n-1} + \alpha F_n$ for $n = 2$. Assume $\alpha^k = F_{k-1} + \alpha F_k$ then $\alpha^{k+1} = \alpha \cdot \alpha^k = \alpha(F_{k-1} + \alpha F_k) = \alpha F_{k-1} + \alpha^2 F_k = \alpha F_{k-1} + (1+\alpha)F_k = F_k + \alpha(F_{k-1} + F_k) = F_k + \alpha F_{k+1}$. Hence $\alpha^n = F_{n-1} + \alpha F_n$ for all $n \geq 2$.

For $n = 10$, $\alpha^{10} = F_9 + \alpha F_{10} = 34 + 55\alpha = 34 + 55\left(\frac{1+\sqrt{5}}{2}\right) = \frac{123+55\sqrt{5}}{2}$.

Chapter 2

4.(a) Let $h = (a, b)$. If $d \mid a$ and $d \mid b$, then $d \mid h$ since $h = ax + by$ for some x, $y \in \mathbb{Z}$. Let $g = (a, b, c)$ and $G = ((a, b), c) = (h, c)$. Since $G \mid h$ and $G \mid c$, and $h \mid a$, $h \mid b$, then $G \mid a$, $G \mid b$, $G \mid c$. Hence $G \leq g$ since g is the greatest of the common divvisors of a, b, and c.

Since $g \mid a$ and $g \mid b$ then $g \mid h$. Since $g \mid c$ also, then $g \leq G$ since G is the greatest common divvisors of h and c. Hence $g = G$.

(b) Since $g = ((a, b), c)$, we can find x_0, $y_0 \in \mathbb{Z}$ such that $g = (a, b)x_0 + cy_0$. Also there exists x_1, $y_1 \in \mathbb{Z}$ such that $(a, b) = ax_1 + by_1$. Then

$$g = (a, b)x_0 + cy_0 = (ax_1 + by_1)x_0 + cy_0 = ax_1x_0 + by_1x_0 + cy_0.$$

(c) We have $g = (17574, 3277, 1365) = ((17574, 3277), 1365)$. Since $29 = (17574, 3277) = 17574(-11) + 3277(59)$ and $g = (29, 1365) = 1 = 29(659) + 1365(-14)$, hence $g = 1 = (17574(-11) + 3277(59))659 + 1365(-14) = 17574(-7249) + 3277(38881) + 1365(-14)$.

5. Using the notation of the Euclidean Algorithm, we have $r_i = r_{i+1}q_{i+2} + r_{i+2}$. We need to prove $r_{i+2} < \frac{1}{2}r_i$.

<u>Case 1</u>: If $r_{i+1} \leq \frac{1}{2}r_i$, then $r_{i+2} < r_{i+1} \leq \frac{1}{2}r_i$.

<u>Case 2</u>: If $r_{i+1} > \frac{1}{2}r_i$, then $q_{i+2} = 1$ for otherwise $q_{i+2} \geq 2$ and then $r_i \geq 2r_{i+1} + r_{i+2} \geq 2r_{i+1}$. Hence $r_{i+1} \leq \frac{1}{2}r_i$ contradicting our assumption. Since then $q_{i+2} = 1$, $r_{i+2} = r_i - r_{i+1} < r_i - \frac{1}{2}r_i = \frac{1}{2}r_i$.

8. We need to find all the non-negative solutions of $6x + 10y + 15z = 167$. Writing the equation in the form $6x + 10y = 167 - 15z$, we observe that z must be odd (why?) and $1 \leq z \leq 9$. For each z, $z = 1, 3, 5, 7, 9$, find the non-negative solutions of $3x + 5y = \frac{167-15z}{2}$.There should be 15 solutions.

11.(a) $22 = 61358(14) + 2090(-411)$. (f) $36 = 7200(-10) + 3132(23)$.

12. $5,829,010$

16.(a) Some hints. Assume $s \geq t$, then there exist integers q and r with $q \geq 1$ and $0 \leq r < t$ such that $s = qt + r$. Then

$$\frac{a^s - 1}{a^t - 1} = \frac{a^{qt+r} - 1}{a^t - 1} = \frac{a^r a^{qt} - a^r + a^r - 1}{a^t - 1} = a^r\left(\frac{(a^t)^q - 1}{a^t - 1}\right) + \frac{a^r - 1}{a^t - 1}.$$

24. $\sqrt{a^2+b^2}$.

25.(iii) $x=-282+37t$, $y=376-49t$, no positive solutions.

(vi) $x=-13+12t$, $y=-13+11t$, infinitely many positive solutions for $t\geq 2$.

26.(g) $x=-102+15t$, $y=51-7t$, $t\in\mathbb{Z}$. The only positive solution is $x=3$, $y=2$.

(i) $x=-7000+24t$, $y=-5000+17t$, $t\in\mathbb{Z}$. There are infinitely many positive solutions, given by $x=80+24t$, $y=15+17t$, for $t\geq 0$.

27.(i) impossible (ii) 5 ways

29. \$10.21

33. 3121 coconuts.

37. The smallest number of people is 63, the largest number is 91.

Chapter 4

3. Since $f(97)\equiv 10 \pmod{11}$, the remainder is 10.

5. The inverse of 1143 modulo 1985 is 1497.

7. By Fermat's (Little) Theorem $n^{16}\equiv 1\equiv a^{16} \pmod{17}$ if $(17,n)=(17,a)=1$. Similarly $n^{16}=(n^4)^4\equiv 1\equiv (a^4)^4\equiv a^{16} \pmod 5$ if $(5,n)=(5,a)=1$. Hence $17\mid (n^{16}-a^{16})$ and $5\mid (n^{16}-a^{16})$. And since $(17,5)=1$, $85\mid (n^{16}-a^{16})$.

13. If p is prime, then $\binom{p}{i}=\frac{p!}{i!(p-i)!}$ is not only an integer for $1\leq i\leq p-1$ but is a multiple of p since p is a factor in the numerator and clearly not a factor in the denominator. Hence

$$\begin{aligned}(k+1)^p &= k^p+\binom{p}{1}k^{p-1}+\binom{p}{2}k^{p-2}+\ldots+\binom{p}{p-1}k+1\\ &\equiv k^p+0+0+\ldots+0+1\\ &\equiv k^p+1 \pmod p.\end{aligned}$$

That is, $(k+1)^p-k^p\equiv 1 \pmod p$. Let a be a positive integer, then adding the congruences

$$(k+1)^p-k^p\equiv 1 \pmod p$$

for $0\leq k\leq a-1$ we have a telescopic sum on the left side resulting in

$$a^p\equiv a \pmod p.$$

(You need to prove also that this result holds even when $a\leq 0$.)

18. If $31\mid (4n^2+4)$, then since $(31,4)=1$, $31\mid (n^2+1)$. Hence $n^2\equiv -1 \pmod{31}$. But this is impossible since $31\not\equiv 1 \pmod 4$.

Chapter 5

1.(n) Since $(7200, 3132) = 36$, we first solve $\frac{7200}{36}x \equiv \frac{3636}{36}(\text{mod } \frac{3132}{36})$; that is, solve $200x \equiv 101(\text{mod } 87)$. Since $200(-10)+87(23) = 1$, a solution is $x = 101(-10) = -1010 \equiv 34(\text{mod } 87)$. Hence the 36 incongruent solutions of $7200x \equiv 3636(\text{mod } 3132)$ are $\{34 + 87k \mid 0 \le k \le 35\}$.

2. The congruences $5x \equiv 9(\text{mod } 16)$, $3x \equiv 1(\text{mod } 13)$, $x \equiv 4(\text{mod } 3)$ are equivalent to

$$\begin{aligned} x &\equiv 5(\text{mod } 16) \quad \ldots(1) \\ x &\equiv 9(\text{mod } 13) \quad \ldots(2) \\ x &\equiv 4(\text{mod } 3) \quad \ldots(3). \end{aligned}$$

From congruence (1), $x = 5 + 16a$ for some $a \in \mathbb{Z}$. From congruence (2), $5 + 16a \equiv 9(\text{mod } 13)$ and hence $a \equiv 10(\text{mod } 13)$. Therefore, $x = 5 + 16a = 5 + 16(10 + 13b) = 165 + 208b$. From (3), $165 + 208b \equiv 4(\text{mod } 3)$ and hence $b \equiv 1(\text{mod } 3)$. Hence $x = 165 + 208b = 165 + 208(1 + 3c) = 373 + 624c$. That is, $x \equiv 373(\text{mod } 624)$.

Chapter 6

7.(a) Given $f(\overline{a}) = (\overline{b}, \overline{c}) = f(\overline{a'})$. Then from the definition of f, $a \equiv b \equiv a'(\text{mod } m)$ and $a \equiv c \equiv a'(\text{mod } n)$. Hence $m \mid (a - a')$ and $n \mid (a - a')$. But $(m, n) = 1$ and hence $mn \mid (a - a')$. Therefore $a \equiv a'(\text{mod } mn)$, so that $\overline{a} = \overline{a'}$. Hence f is one-to-one.

Let $(\overline{b}, \overline{c}) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$. The Chinese Remainder Theorem says that there is a common solution $x = a$ for the congruences $x \equiv b(\text{mod } m)$ and $x \equiv c(\text{mod } n)$ since $(m, n) = 1$. Hence $f(\overline{a}) = (\overline{b}, \overline{c})$ so that f is also onto.

(b) Since f is one-to-one and onto the number of elements in the set $\mathbb{Z}_{mn}^*$ is the same as that of $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$. The former has $\phi(mn)$ elements and the latter has $\phi(m)\phi(n)$ elements.

10. A hint for this problem is to note that

$$\prod_{\substack{2 \le p \le 19 \\ p \text{ prime}}} (1 - \frac{1}{p}) = \frac{55296}{323323} > \frac{1}{6}.$$

15. Let $x = 7^{9999}$. Note that $\phi(1000) = 1000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 400$. Hence by Fermat's (Little) Theorem

$$7x = 7^{10000} = \left(7^{\phi(1000)}\right)^{25} \equiv 1^{25} \equiv 1(\text{mod } 1000).$$

Since $7(143)+1000(-1) = 1$, then $143(7) \equiv 1 (\bmod 1000)$. Hence $x \equiv 143 (\bmod 1000)$, and so the last three digits in x are 1, 4, 3.

22.(a) We are given that $a^h \equiv 1 (\bmod p)$ and hence $p \mid (a^h - 1)$. That is,

$$p \mid (a^{\frac{h}{2}} - 1)(a^{\frac{h}{2}} + 1).$$

Since p is prime then $p \mid (a^{\frac{h}{2}} - 1)$ or $p \mid (a^{\frac{h}{2}} + 1)$. But $a^{\frac{h}{2}} \not\equiv 1 (\bmod p)$ since h is the smallest positive exponent such that $a^h \equiv 1 (\bmod p)$. Hence $p \mid (a^{\frac{h}{2}} + 1)$ and so $a^{\frac{h}{2}} \equiv -1 (\bmod p)$.

(b) For $p = 2$ the result is trivial. Assume that p is an odd prime and let g be a primitive root modulo p. (We assume that g exists, but we have not proved this!) Hence $g^{p-1} \equiv 1 (\bmod p)$ and $p - 1$ is the order of g modulo p. Hence by part(a) $g^{\frac{p-1}{2}} \equiv -1 (\bmod p)$. We have

$$(p-1)! \equiv \prod_{i=1}^{p-1} g^i = g^{\sum_{i=1}^{p-1} i} = g^{\frac{(p-1)p}{2}} = \left(g^{\frac{p-1}{2}}\right)^p \equiv (-1)^p = -1 (\bmod p).$$