Chapter 1

Integers and Permutations

1.1 INDUCTION

1. In each case we give the equation that makes p_k imply p_{k+1}.
   (a) $k(2k-1)+(4k+1)=2k^2+3k+1=(k+1)(2k+1)$
   (c) $\frac{1}{4}k^2(k+1)^2+(k+1)^3=\frac{1}{4}(k+1)^2(k^2+4k+4)=\frac{1}{4}(k+1)^2(k+2)^2$
   (e) $\frac{1}{12}k(k+1)(k+2)(3k+5)+(k+1)(k+2)^2$
   $=\frac{1}{12}(k+1)(k+2)(3k^2+17k+24)=\frac{1}{12}(k+1)(k+2)(k+3)(3k+8)$
   (g) $\frac{k}{3}(4k^2-1)+(2k+1)^2=\frac{k}{3}(2k-1)(2k+1)+(2k+1)^2$
   $=\frac{1}{3}(2k+1)[2k^2+5k+3]=\frac{1}{3}(2k+1)(k+1)(2k+3)$
   $=\frac{1}{3}(k+1)[4(k+1)^2-1]$
   (i) $1-\frac{1}{(k+1)!}+\frac{k+1}{(k+2)!}=1-\frac{1}{(k+2)!}[(k+2)-(k+1)]=1-\frac{1}{(k+2)!}$
2. In each case we give the inequality that makes p_k imply p_{k+1}.
   (a) $2^{k+1}=2\cdot 2^k>2\cdot k\geq k+1$.
   (c) If $k!\leq 2^{k^2}$, then $(k+1)!=(k+1)k!\leq(k+1)2^{k^2}\leq 2^{(k+1)^2}$ provided $k+1\leq 2^{2k+1}$. This latter inequality follows, again by induction on $k\geq 1$, because $2^{2k+3}=4\cdot 2^{2k+1}\geq 4(k+1)\geq k+2$.
   (e) $\frac{1}{\sqrt{1}}+\cdots+\frac{1}{\sqrt{k}}+\frac{1}{\sqrt{k+1}}\geq\sqrt{k}+\frac{1}{\sqrt{k+1}}=\frac{\sqrt{k^2+k}+1}{\sqrt{k+1}}\geq\frac{k+1}{\sqrt{k+1}}=\sqrt{k+1}$.
3. In each case we give the calculation that makes p_k imply p_{k+1}.
   (a) If $k^3+(k+1)^3+(k+2)^3=9m$, then
   $(k+1)^3+(k+2)^3+(k+3)^3=9m-k^3+(k+3)^3=9m+9k^2+27k+27$.
   (c) If $3^{2k+1}+2^{k+2}=7m$, then

$$3^{2k+3}+2^{k+3}=9(7m-2^{k+2})+2^{k+3}=9\cdot 7m-2^{k+2}(9-2).$$

Student Solution Manual to Accompany Introduction to Abstract Algebra, Fourth Edition.
W. Keith Nicholson.

5. If $3^{3k}+1=7m$ where k is odd, then passing to $k+2$,
$$\begin{aligned} 3^{3(k+2)}+1 = 3^6(7m-1)+1 &= 3^6\cdot 7m-(3^6-1) \\ &= 3^6\cdot 7m-728=7(3^6\cdot m-104). \end{aligned}$$

7. It is clear if $n=1$. In general, such a $(k+1)$ digit number must end in 4, 5 or 6, and there are 3^k of each by induction. We are done since $3\cdot 3^k=3^{k+1}$.

9. It is clear if $n=1$. Given $k+1$ secants, remove one and color the result unambiguously by induction. Now reinsert the removed secant. On one side of this secant, leave all regions the original color (including the new regions of that side created by the new secant). On the other side, interchange colors everywhere (including those regions newly created). This is an unambiguous coloring.

10. (a) If $k\geq 2$ cents can be made up, there must be a 2-cent or a 3-cent stamp. In the first case, replace a 2-cent stamp by a 3-cent stamp; in the second case, replace a 3-cent stamp by two 2-cent stamps.

    (c) If $k\geq 18$ can be made up, either one 7-cent stamp is used (replace with two 4-cent stamps) or five 4-cent stamps are used (replace with three 7-cent stamps).

11. $a_0=0$, $a_1=7$, $a_2=63=7.9$, $a_3=511=7\cdot 73$. The conjecture is that $2^{3n}-1$ is a multiple of 7 for all $n\geq 0$. If $2^{3k}-1=7x$ for some $n\geq 0$, then we have $2^{3(k+1)}-1=2^3(7x+1)-1=7(2^3+1)$.

12. (a) If S_n is the statement "$1^3+2^3+3^3+\cdots+n^3$ is a perfect square", then S_1 is true. If $k\geq 1$, assume that $1^3+2^3+\cdots+k^3=x^2$ for some integer x. Then $1^3+2^3+\cdots+(k+1)^3=x^2+(k+1)^3$ and it is not clear how to deduce that this is a perfect square without some knowledge about how x is dependent upon k. Thus induction fails for S_n. However, if we strengthen the statement to $1^3+2^3+\cdots+n^3=\left[\frac{1}{2}n(n+1)\right]^2$, induction *does* go through (see Exercise 1(c)). The reason is that now the inductive hypothesis brings more information to the inductive step and so allows the (stronger) conclusion to be deduced.

13. $\binom{n}{r-1}+\binom{n}{r}=\frac{n!}{(r-1)!(n-r+1)!}+\frac{n!}{r!(n-r)!}=\frac{n!}{r!(n+1-r)!}[r+(n+1-r)]=\binom{n+1}{r}$.

14. (a) $\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{n}=(1+1)^n=2^n$ by the binomial theorem (Example 6 with $x=1$).

15. We use the well-ordering principle to prove the principle of induction. Let $p_1,p_2,p_3,\cdots$ be statements such that p_1 is true and $p_k\Rightarrow p_{k+1}$ for every $k\geq 1$. We must show that p_n is true for every $n\geq 1$. To this end consider the set $X=\{n\geq 1\mid p_n \text{ is false}\}$; we must show that X is empty. But if X is nonempty it has a smallest member m by the well-ordering principle. Hence $m\neq 1$ (because p_1 is true), so $m-1$ is a positive integer. But then p_{m-1} is true (because m is the *smallest* member of X) and so p_m is true (because $p_{m-1}\Rightarrow p_m$). This contradiction shows that X must be empty, as required.

17. If p_n is "n has a prime factor", then p_2 is true. Assume $p_2,\ldots,p_k$ are all true. If $k+1$ is a prime, we are done. If $k+1=ab$ write $2\leq a\leq k$ and $2\leq b\leq k$, then a (and b) has a prime factor by strong induction. Thus $k+1$ has a prime factor.

18. (a) $a_n = 2(-1)^n \qquad a_{n+1} = -a_n = -2(-1)^n = 2(-1)^{n+1}$

    (c) $a_n = \frac{1}{2}[1 + (-1)^n]$
    $a_{n+1} = 1 - a_n = 1 - \frac{1}{2}[1 + (-1)^n] = \frac{1}{2}[2 - 1 - (-1)^n] = \frac{1}{2}[1 + (-1)^{n+1}]$

19. Given n lines, another line intersects all existing lines (because no two are parallel) at new intersection points (none of these are concurrent) and so enters $n + 1$ regions. Hence it creates $n + 1$ new regions; so $a_{n+1} = a_n + (n + 1)$. Then $a_0 = 1$, $a_1 = 1 + 1$, $a_2 = 1 + 1 + 2$, $a_3 = 1 + 1 + 2 + 3$; and this suggests $a_n = 1 + (1 + 2 + \cdots + n)$. Hence Gauss' formula (Example 1) gives

$$a_n = 1 + \tfrac{1}{2}n(n + 1) = \tfrac{1}{2}(n^2 + n + 2).$$

    This is valid for $n = 0$; if it holds for $n = k \geq 1$ then

$$a_{k+1} = a_k + (k + 1) = \tfrac{1}{2}[(k^2 + k + 2) + 2(k + 1)] = \tfrac{1}{2}[(k + 1)^2 + (k + 1) + 2].$$

21. (a) Let p_n denote the statement $a_n = (-1)^n$. Then p_0 and p_1 are true by hypothesis. If p_k and p_{k+1} are true for some $k \geq 0$, then $a_k = (-1)^k$, $a_{k+1} = (-1)^{k+1}$ and so

$$a_{k+2} = a_{k+1} + 2a_k = (-1)^{k+1} + 2(-1)^k = (-1)^k[-1 + 2] = (-1)^k = (-1)^{k+2}.$$

    Thus p_{k+2} is true and the principle applies.

23. $p_1 \Rightarrow p_2$ fails.

24. (a) Prove p_1 and p_2 are true.

25. If p_k is true for some k, then $p_{k-1}, p_{k-2}, \ldots, p_1$ are all true by induction using the first condition. Given m, the second condition implies that p_k is true for some $k \geq m$, so p_m is true.

27. (a) Apply the recursion theorem with $s_0 = a_0$ and $s_n = s_{n-1} + a_n$.

1.2 DIVISORS AND PRIME FACTORIZATION

1. (a) $391 = 23 \cdot 17 + 0 \qquad$ (c) $-116 = (-9) \cdot 13 + 1$

2. (a) $n/d = 51837/386 = 134.293$, so $q = 134$. Thus $r = n - qd = 113$.

3. If $d > 0$, then $|d| = d$ and this is the division algorithm. If $d < 0$, then $|d| = -d > 0$ so $n = q(-d) + r = (-q)d + r$, $0 \leq r \leq |d|$.

5. Write $m = 2k + 1$, $n = 2j + 1$. Then $m^2 - n^2 = 4[k(k + 1) - j(j + 1)]$. But each of $k(k + 1)$ and $j(j + 1)$ is even, so $8 \mid (m^2 - n^2)$.

7. (a) $10(11k + 4) - 11(10k + 3) = 7$, so $d \mid 7$. Thus $d = 1$ or $d = 7$.

9. (a) $72 = 42 + 30$
    $42 = 30 + 12$
    $30 = 2 \cdot 12 + 6$
    $12 = 2 \cdot 6$
    Thus, $\gcd(72, 42) = 6$ and
    $6 = 30 - 2(42 - 30)$
    $= 3 \cdot 30 - 2 \cdot 42$
    $= 3(72 - 42) - 2 \cdot 42$
    $= 3 \cdot 72 - 5 \cdot 42$

    (c) $327 = 6 \cdot 54 + 3$
    $54 = 3 \cdot 18$
    Thus $\gcd(327 \cdot 54) = 3$ and
    $3 = 1 \cdot 327 - 6 \cdot 54$

(e) $377 = 13 \cdot 29$

Hence $29 \mid 377$, so

$\gcd(29, 377) = 29$. Thus

$29 = 0 \cdot 377 + 1 \cdot 29$

(g) $72 = 0 \cdot (-176) + 72$

$-175 = (-3) \cdot 72 + 41$

$72 = 41 + 31$

$41 = 31 + 10$

$31 = 3 \cdot 10 + 1$

Hence $\gcd(72, -175) = 1$ and

$1 = 31 - 3(41 - 31)$

$= 4(72 - 41) - 3 \cdot 41$

$= 4 \cdot 72 - 7(-175 + 3 \cdot 72)$

$= (-17) \cdot 72 - 7 \cdot (-175)$

11. If $m = qd$, then $\frac{m}{k} = q\frac{d}{k}$, so $\frac{d}{k} \mid \frac{m}{k}$. Similarly, $\frac{d}{k} \mid \frac{n}{k}$. If $d = xm + yn$, then $\frac{d}{k} = x\frac{m}{k} + y\frac{n}{k}$, so any common divisor of $\frac{m}{k}$ and $\frac{n}{k}$ is a divisor of $\frac{d}{k}$.

13. It is prime for $n = 1, 2, \dots, 9$; but $10^2 + 10 + 11 = 121 = 11^2$.

15. If $d = \gcd(m, n)$ and $d_1 = \gcd(m_1, n_1)$, then $d \mid m$ and $d \mid n$, so $d \mid m_1$ and $d \mid n_1$ by hypothesis. Thus $d \mid d_1$.

17. If $1 = xm + yn$ and $1 = x_1k + y_1n$, then

$$1 = (xm + yn)(x_1k + y_1n) = (xx_1)mk + (xmy_1 + yx_1k + yny_1)n.$$

Thus $\gcd(mk, n) = 1$ by Theorem 4.

Alternatively, if $d = \gcd(mk, n) \neq 1$ let $p \mid d$, p a prime. Then $p \mid n$ and $p \mid mk$ But then $p \mid m$ or $p \mid k$, a contradiction either way because we have $\gcd(m, n) = 1 = \gcd(m, n)$.

19. Write $d = \gcd(m, n)$ and $d' = \gcd(km, kn)$. We must show $kd = d'$. First, $d \mid m$ and $d \mid n$, so $kd \mid km$ and $kd \mid kn$. Hence, $kd \mid d'$. On the other hand, write $km = qd'$ and $kn = pd'$. We have $d = xm + yn$, $x, y \in \mathbb{Z}$, so

$$kd = xkm + ykn = xqd' + ypd'.$$

Thus $d' \mid kd$. As $k \geq 1$ it follows that $d' = kd$.

21. If p is not a prime, then assume $p = mn$ with $m \geq 2$ and $n \geq 2$. But then $p \mid m$ or $p \mid n$ by hypothesis, so $p \leq m < p$ or $p \leq n < p$, a clear contradiction.

23. No. If $a = 18$ and $n = 12$ then $d = 6$ so $\frac{a}{d} = 3$ is not relatively prime to $n = 12$.

25. Let them be $2k + 1$, $2k + 3$, $2k + 5$. We have $k = 3q + r$, $r = 0, 1, 2$. If $r = 0$ then $3 \mid (2k + 3)$; if $r = 1$, then $3 \mid (2k + 1)$; and if $r = 2$, then $3 \mid (2k + 5)$. Thus one of these primes is a multiple of 3, and so is 3.

27. Let $d = \gcd(m, p^k)$, then $d \mid m$ and $d \mid p^k$. Thus $d = p^j$, $j \leq k$. If $j > 0$, then $p \mid d$, so (since $d \mid m$) $p \mid m$. This contradicts $\gcd(m, p) = 1$. So $j = 0$ and $d = 1$.

29. We have $a \mid a_1b_1$ and $(a, b_1) = 1$. Hence $a \mid a_1$ by Theorem 5. Similarly $a_1 \mid a$, so $a = a_1$ because both are positive. Similarly $b = b_1$.

30. (a) $27783 = 3^4 \cdot 7^3$

(c) $2431 = 11 \cdot 13 \cdot 17$

(e) $241 = 241$ (a prime)

31. (a) $735 = 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^2 \cdot 11^0$ and $110 = 2^1 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 11^1$. Hence

$$\gcd(735, 110) = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^2 \cdot 11^0 = 5, \text{ and}$$

$$\operatorname{lcm}(735, 110) = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^2 \cdot 11^1 = 16170.$$

(c) $139 = 2^0 \cdot 139^1$ and $278 = 2^1 \cdot 139^1$. Hence

$$\gcd(139, 278) = 2^0 \cdot 139^1 = 139, \text{ and } \operatorname{lcm}(139, 278) = 2^1 \cdot 139^1 = 278.$$

33. (a) Use Theorem 8. In forming $d = p_1^{d_1} \dots p_r^{d_r}$, there are $(n_1 + 1)$ choices for d_1 among $0, 1, 2, \dots, n_i$; then there are $(n_2 + 1)$ choices for d_2 among $0, 1, 2, \dots, n_2$; and so on. Thus there are $(n_1 + 1)(n_2 + 1) \cdots (n_r + 1)$ choices in all, and each leads to a different divisor by the uniqueness in the prime factorization theorem.

35. Let $m = p_1^{m_1} \dots p_r^{m_r}$ and $n = q_1^{n_1} \dots q_s^{n_s}$ be the prime factorizations of m and n. Since $\gcd(m, n) = 1$, $p_i \neq q_j$ for all i and j, so the prime factorization of mn is $mn = p_1^{m_1} \dots p_r^{m_r} q_1^{n_1} \dots q_s^{n_s}$. Since $d \mid mn$, we have $d = p_1^{d_1} \dots p_r^{d_r} q_1^{e_1} \dots q_s^{e_s}$ where $0 \leq d_i \leq m_i$ for each i and $0 \leq e_j \leq n_j$ for each j. Take $m_1 = p_1^{d_1} \dots p_r^{d_r}$ and $n_1 = q_1^{e_1} \dots q_s^{e_s}$.

37. Write $a = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ and $b = p_1^{b_1} p_2^{b_2} \dots p_r^{b_r}$ where the p_i are distinct primes, $a_i \geq 0$ and $b_i \geq 0$. Let $u_i = \begin{cases} 0 & \text{if } a_i < b_i \\ a_i & \text{if } a_i \geq b_i \end{cases}$ and $v_i = \begin{cases} b_i & \text{if } a_i < b_i \\ 0 & \text{if } a_i \geq b_i \end{cases}$, and then take $u = p_1^{u_1} p_2^{u_2} \dots p_r^{u_r}$ and $v = p_1^{v_1} p_2^{v_2} \dots p_r^{v_r}$. Then $u \mid a$, $v \mid b$ and $\gcd(u, v)$=1. Moreover $uv = \operatorname{lcm}(a, b)$ by Theorem 9 because $u_i + v_i = \max(a_i, b_i)$ for each i.

39. (a) By the division algorithm, $p = 4k + r$ for $r = 0, 1, 2$ or 3. But $r = 0$ or 2 is impossible since p is odd (being a prime greater than 2).

41. (a) $28665 = 3^2 \cdot 5^1 \cdot 7^2 \cdot 11^0 \cdot 13^1$ and $22869 = 3^3 \cdot 5^0 \cdot 7^1 \cdot 11^2 \cdot 13^0$ so,

$$\gcd(28665, 22869) = 3^2 \cdot 5^0 \cdot 7^1 \cdot 11^0 \cdot 13^0 = 63$$
$$\operatorname{lcm}(28665, 22869) = 3^3 \cdot 5^1 \cdot 7^2 \cdot 11^2 \cdot 13^1 = 10,405,395$$

43. Let $X = \{x_1 a_1 + \cdots + x_k a_k \mid x_i \in \mathbb{Z},\ x_1 a_1 + \cdots + x_k a_k \geq 1\}$. Then $X \neq \varnothing$ because $a_1^2 \cdots + a_k^2 \in X$, so let m be the smallest member of X. Then $m = x_1 a_1 + \cdots + x_k a_k$ for integers a_k, so we show $d = m$. Since $d \mid a_i$ for each i, it is clear that $d \mid m$. We can show $m \mid d$, if we can show that m is a common divisor of the a_i (by definition of $d = \gcd(a_1, \cdots, a_k)$). Write $a_1 = qm + r$, $0 \leq r < m$. Then

$$r = a_1 - qm = (1 - qx_1)a_1 + (-qx_2)a_2 + \cdots + (-qx_k)a_k,$$

and this contradicts the minimality if $r \geq 1$. So $r = 0$ and $m \mid a_1$. A similar argument shows $m \mid a_i$ for each i.

45. (a) Let $m = qn + r$, $0 \leq r < n$. If $m < n$, then $q = 0$ and $r = m$. If $m \geq n$, then $q \geq 1$. Thus $q \geq 0$. We want $x \in \mathbb{Z}$ such that $2^m - 1 = x(2^n - 1) + (2^r - 1)$. Solving for x (possibly in $\mathbb{Q}$):

$$x = \frac{2^m - 2^r}{2^n - 1} = 2^r \left(\frac{2^{m-r} - 1}{2^n - 1} \right) = 2^r \left(\frac{(2^n)^q - 1}{2^n - 1} \right).$$

If $q = 0$, take $x = 2^r = 2^m$; if $q > 0$, take $x = (2^n)^{q-1} + \cdots + 2^n + 1$.

1.3 INTEGERS MODULO n

1. (a) True. $40 - 13 = 3 \cdot 9$

   (c) True. $-29 - 6 = (-5)7$

   (e) True. $8 - 8 = 0 \cdot n$ for any n.

   (g) False. $8^4 \equiv (64)^2 \equiv (-1)^2 \equiv 1 \pmod{13}$.

2. (a) $2k - 4 = 7q$, so q is even. Thus $k = 2 + 7x$ for some integer x; that is $k \equiv 2 \pmod 7$.

   (c) $2k \equiv 0 \pmod 9$, so $2k = 9q$. Thus $2 \mid q$, so $k = 9x$ for some integer x; that is $k \equiv 0 \pmod 9$.

3. (a) $10 \equiv 0 \pmod k$, so $k \mid 10$: $k = 2, 5, 10$.

   (c) $k^2 - 3 = qk$, so $k \mid 3$. Thus $k = 1, 3$ so, (as $k \geq 2$ by assumption) $k = 3$.

5. (a) $a \equiv b \pmod 0$ means $a - b = q \cdot 0$ for some q, that is $a = b$.

6. (a) $a \equiv a$ for all a because $n \mid (a - a)$. Hence if $n \mid (a - b)$, then $n \mid (b - a)$. Hence if $a - b = xn$ and $b - c = yn$, $x, y \in \mathbb{Z}$, then $a - c = (x + y)n$.

7. If $n = pm$ and $a \equiv b (\bmod n)$, then $a - b = qn = qpm$. Thus $a \equiv b (\bmod m)$.

8. (a) In $\mathbb{Z}_7 : \overline{10} = \bar{3}$, so $\overline{10}^2 = \bar{9} = \bar{2}$, $\overline{10}^3 = \bar{6} = \overline{-1}$, $\overline{10}^6 = \bar{1}$. Since $515 = 6 \cdot 85 + 5$ we get $\overline{10}^{515} = (\overline{10}^6)^{85} \cdot \overline{10}^5 = \bar{1}^{85} \cdot \overline{10}^2 \cdot \overline{10}^3 = \bar{2} \cdot \overline{(-1)} = \bar{5}$. Hence $10^{515} \equiv 5 (\bmod 7)$.

9. (a) In $\mathbb{Z}_{10} : \bar{3}^2 = \bar{9} = -1$, so $\bar{3}^4 = \bar{1}$. Since $1027 = 4 \cdot 256 + 3$, we get $\bar{3}^{1027} = (\bar{3}^4)^{256} \cdot \bar{3}^3 = \bar{1}^{256} \cdot \overline{27} = \bar{7}$. The unit decimal is 7.

11. $\bar{p} = \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$ in $\mathbb{Z}_6$. If $\bar{p} = \bar{0}, \bar{2}, \bar{4}$ then $2 \mid p$; if $\bar{p} = \bar{3}$, then $3 \mid p$. So $\bar{p} = \bar{1}$ or $\bar{p} = \bar{5}$.

12. (a) $\bar{a} = \bar{0}, \bar{1}, \bar{2}, \bar{3}$ in $\mathbb{Z}_4$, so $\bar{a}^2 = \bar{0}, \bar{1}, \bar{0}, \bar{1}$ respectively.

13. $\bar{a} = \bar{0}, \bar{1}, \ldots, \overline{10}$ in $\mathbb{Z}_{11}$. Taking each case separately:

$$\begin{array}{ll}
\bar{0}^5 = \bar{0} & \bar{6}^5 = \overline{(-5)}^5 = \overline{-5}^5 = \overline{-1} \\
\bar{1}^5 = \bar{1} & \bar{7}^5 = \overline{(-4)}^5 = \overline{-4}^5 = \overline{-1} \\
\bar{2}^5 = \overline{32} = \overline{-1} & \bar{8}^5 = \overline{(-3)}^5 = \overline{-3}^5 = \overline{-1} \\
\bar{3}^5 = \bar{9} \cdot \overline{27} = \bar{9} \cdot \bar{5} = \bar{1} & \bar{9}^5 = \overline{(-2)}^5 = \overline{-2}^5 = \bar{1} \\
\bar{4}^5 = \overline{16} \cdot \overline{64} = \bar{5} \cdot \bar{9} = \bar{1} & \overline{10}^5 = \overline{(-1)}^5 = \overline{-1} \\
\bar{5}^5 = \overline{25} \cdot \overline{25} \cdot \bar{5} = \bar{3} \cdot \bar{3} \cdot \bar{5} = \bar{1} &
\end{array}$$

15. One of $a, a+1$ must be even so $2 \mid a(a+1)(a+2)$; similarly, one of a, $a+1, a+2$ is a multiple of 3 [in fact $a \equiv 0$ means $3 \mid a$, $a \equiv 1$ means $3 \mid a+2$, and $a \equiv 2$ means $3 \mid a+1$]. Hence $3 \mid a(a+1)(a+2)$. But 2 and 3 are relatively prime so $2 \cdot 3 = 6$ also divides $a(a+1)(a+2)$. Hence

$$\bar{a}(\bar{a} + \bar{1})(\bar{a} + \bar{2}) = \overline{a(a+1)(a+2)} = \bar{0} \text{ in } \mathbb{Z}_6.$$

17. Since $\bar a = \bar 0, \bar 1, \dots, \bar 5$ in $\mathbb{Z}_6$, we examine every case.

$$\begin{array}{ll} \bar 0^3 = \bar 0 & \bar 3^3 = \overline{27} = \bar 3 \\ \bar 1^3 = \bar 1 & \bar 4^3 = \overline{(-2)}^3 = -(\bar 2)^3 = \overline{-2} = \bar 4 \\ \bar 2^3 = \bar 8 = \bar 2 & \bar 5^3 = \overline{(-1)}^3 = \overline{-1} = \bar 5 \end{array}$$

Hence $\bar a^3 = \bar a$ in all cases.

18. (a) Since $\bar a = \bar 0, \bar 1, \dots, \bar 4$ in $\mathbb{Z}_5$, it suffices to show each of these is a cube in $\mathbb{Z}_5$. Look at the cubes in $\mathbb{Z}_5 : \bar 0^3 = \bar 0$, $\bar 1^3 = \bar 1$, $\bar 2^3 = \bar 3$, $\bar 3^3 = \bar 2$, and $\bar 4^3 = \overline{(-1)}^3 = -\bar 1 = \bar 4$. Thus every residue $\bar 0, \bar 1, \bar 2, \bar 3, \bar 4$ is a cube in $\mathbb{Z}_5$.

19. (a) Since $\bar k = \bar 0, \bar 1, \bar 2, \bar 3, \bar 4, \bar 5, \bar 6$ in $\mathbb{Z}_7$, we get $\bar k^2 + \bar 1 = \bar 1, \bar 2, \bar 5, \bar 3, \bar 3, \bar 5, \bar 2$ respectively. Clearly $\bar k^2 + \bar 1 = \bar 0$ does not occur in $\mathbb{Z}_7$.

21. We have $n = d_0 + 10d_1 + 10^2 d_2 + \cdots + 10^k d_k$.

(a) $\overline{10} = \bar 1$ in $\mathbb{Z}_3$, so $\bar n = \overline{d_0} + \bar 1 \cdot \overline{d_1} + \bar 1^2 \overline{d_2} + \cdots + \bar 1^k d_k = \overline{d_0 + d_1 + \cdots + d_k}$. Thus $\bar n = \overline{d_0} + \overline{d_1} + \cdots + \overline{d_k} (\text{mod}\, 3)$.

22. (a) By the euclidean algorithm,
$$\begin{array}{lcl} 35 = 2 \cdot 13 + 9 & & 1 = 9 - 2(13 - 9) \\ 13 = 1 \cdot 9 + 4 & \text{so} & = 3(35 - 2 \cdot 13) - 2 \cdot 13\,. \\ 9 = 2 \cdot 4 + 1 & & = 3 \cdot 35 - 8 \cdot 13 \end{array}$$
Hence $(-8) \cdot 13 \equiv 1 (\text{mod}\, 35)$, so $\overline{-8} = \overline{27}$ is the inverse of $\overline{13}$ in $\mathbb{Z}_{35}$. Then $\overline{13} \cdot \bar x = \bar 9$ gives $\bar x = \overline{27} \cdot \overline{13} \cdot \bar x = \overline{27} \cdot \bar 9 = \overline{-8} \cdot \bar 9 = \overline{-72} = \overline{-2} = \overline{33}$.

(c) Euclidean algorithm:
$$\begin{array}{lcl} 20 = 11 + 9 & & 1 = 9 - 4(11 - 9) \\ & & = 5 \cdot 9 - 4 \cdot 11 \\ 11 = 9 + 2 & \text{so} & = 5(20 - 11) - 4 \cdot 11 \\ 9 = 4 \cdot 2 + 1 & & = 5 \cdot 20 - 9 \cdot 11 \end{array}.$$
Hence the inverse of $\overline{11}$ is $\overline{-9} = \overline{11}$, so $\overline{11} \cdot \bar x = \overline{16}$ gives $\bar x = \overline{11} \cdot \overline{16} = \overline{16}$.

23. (a) Let $\bar d$ be the inverse of $\bar a$ in $\mathbb{Z}_n$, so $\bar d \cdot \bar a = \bar 1$ in $\mathbb{Z}_n$, then multiply $\bar a \cdot \bar b = \bar a \cdot \bar c$ by $\bar d$ to get $\bar d \cdot \bar a \cdot \bar b = \bar d \cdot \bar a \cdot \bar c$, that is $\bar 1 \cdot \bar a = \bar 1 \cdot \bar c$, that is $\bar a = \bar c$.

24. (a) If $\bar c$ and $\bar d$ are the inverses of $\bar a$ and $\bar b$ respectively in $\mathbb{Z}_n$, then $\bar c \cdot \bar a = \bar 1$ and $\bar d \cdot \bar b = \bar 1$. Multiplying, we find $\bar c \cdot \bar a \cdot \bar d \cdot \bar b = \bar 1$, that is $(\bar c \cdot \bar d)(\bar a \cdot \bar b) = \bar 1$. Hence $\bar c \cdot \bar d$ is the inverse of $\bar a \cdot \bar b = \overline{ab}$ in $\mathbb{Z}_n$.

25. (a) Multiply equation 2 by $\bar 2$ to get $\overline{10}x + \bar 2y = \bar 2$. Subtract this from equation 1: $\bar 7x = \bar 1$. But $\bar 8 \cdot \bar 7 = \bar 1$ in $\mathbb{Z}_{11}$, so $x = \bar 8 \cdot \bar 1 = \bar 8$. Then equation 2 gives $y = \bar 1 - \bar 5 \cdot \bar 8 = \bar 5$.

(c) Multiply equation 2 by $\bar 2$ to get $\bar 3x + \bar 2y = \bar 2$. Comparing this with the first equation gives $\bar 1 = \bar 3x + \bar 2y = \bar 2$, an impossibility. So there is no solution to these equations in $\mathbb{Z}_7$. (Compare with (a)).

(e) Multiply equation 2 by $\bar 2$ to get $\bar 3x + \bar 2y = \bar 1$, which is just equation 1. Hence, we need only solve equation 2. If $x = \bar r$ is arbitrary in $\mathbb{Z}_7$ (so $\bar r = \bar 0, \bar 1, \dots, \bar 6$), then $y = \bar 4 - \bar 5x = \overline{4 - 5r}$. Thus the solutions are:

x	$\bar 0$	$\bar 1$	$\bar 2$	$\bar 3$	$\bar 4$	$\bar 5$	$\bar 6$
y	$\bar 4$	$\bar 6$	$\bar 1$	$\bar 3$	$\bar 5$	$\bar 0$	$\bar 2$

.

27. If an expression $x^2 + ax$ is given where a is a number, we can *complete the square* by adding $\left(\frac{1}{2}a\right)^2$. Then $x^2 + ax + \left(\frac{1}{2}a\right)^2 = (x + \frac{1}{2}a)^2$. The same thing works in $\mathbb{Z}_n$ except $\frac{1}{2}$ is replaced by the inverse of $\bar{2}$ if it exists.

    (a) $x^2 + \bar{5}x + \bar{4} = \bar{0}$ means $x^2 + \bar{5}x = \bar{3}$ in $\mathbb{Z}_7$. The inverse of $\bar{2}$ is $\bar{4}$ in $\mathbb{Z}_7$, so the square is completed by adding $(\bar{4} \cdot \bar{5})^2 = \bar{1}$ to both sides. The result is

    $$(x + \bar{6})^2 = x^2 + \bar{5}x + \bar{1} = \bar{3} + \bar{1} = \bar{4}.$$

    The only members of $\mathbb{Z}_7$ which square to $\bar{4}$ are $\bar{2}$ and $\overline{-2} = \bar{5}$. (See Exercise 26.) Hence $x + \bar{6} = \bar{2}$ or $\bar{5}$; that is $x = \bar{3}$ or $\bar{6}$.

    (c) $x^2 + x + \bar{2} = \bar{0}$ gives $x^2 + x = \bar{3}$ in $\mathbb{Z}_5$. The inverse of $\bar{2}$ is $\bar{3}$ in $\mathbb{Z}_5$, so add $\bar{3}^2 = \bar{4}$ to both sides

    $$(x + \bar{3})^2 = x^2 + x + \bar{4} = \bar{3} + \bar{4} = \bar{2}.$$

    But $\bar{2}$ is not a square in $\mathbb{Z}_5$ $[\bar{0}^2 = \bar{0},\ \bar{1}^2 = \bar{4}^2 = \bar{1},\ \bar{2}^2 = \bar{3}^2 = \bar{4}]$, so there is no solution.

    (e) Since n is odd, $\gcd(2, n) = 1$, so $\bar{2}$ has an inverse in $\mathbb{Z}_n$; call it $\bar{r}$. Now $x^2 + \bar{a}x + \bar{b} = \bar{0}$ in $\mathbb{Z}_n$ means $x^2 + \bar{a}x = \overline{-b}$. Complete the square by adding $(\bar{r} \cdot \bar{a})^2 = \overline{ra}^2$ to both sides. The result is

    $$(x + \overline{ra})^2 = x^2 + \bar{a} + ra^2 = -b + ra^2 = (\bar{r}^2\bar{a}^2 - \bar{b}).$$

    Thus, there is a solution if and only if $(\bar{r}^2\bar{a}^2 - \bar{b})$ is a square in $\mathbb{Z}_n$.

29. (a) Let $\bar{a} \cdot \bar{b} = \bar{0}$ in $\mathbb{Z}_n$. If $\gcd(a, n) = 1$, then a has an inverse in $\mathbb{Z}_n$, say $\bar{c} \cdot \bar{a} = \bar{1}$. Then $\bar{b} = \bar{1}\,\bar{b} = \bar{c} \cdot \bar{a} \cdot \bar{b} = \bar{c} \cdot \bar{0} = \bar{0}$.

31. (1) $\Rightarrow$ (2). Assume (1) holds but n is not a power of a prime. Then $n = p^k a$ where p is a prime, $k \geq 1$, and $a > 1$ has $p \nmid a$. Then $\gcd(n, a) = a > 1$, so $\bar{a}$ has no inverse in $\mathbb{Z}_n$. But $\bar{a}^n \neq \bar{0}$ too. In fact $\bar{a}^n = \bar{0}$ means $n \mid a^n$ whence $p \mid a^n$. By Euclid's lemma, this implies $p \mid a$, contrary to choice.

33. In $\mathbb{Z}_{223}$, $\bar{2}^8 = \overline{256} = \overline{33}$. Thus $\bar{2}^{16} = \overline{33}^2 = \overline{197}$, $\bar{2}^{32} = \overline{197}^2 = \bar{7}$, and finally $\bar{2}^{37} = \bar{2}^{32} \cdot \bar{2}^5 = \bar{7} \cdot \overline{32} = \overline{224} = \bar{1}$. Similarly, in $\mathbb{Z}_{641}$,

    $$\bar{2}^8 = \overline{256},\ \bar{2}^{16} = \overline{256}^2 = \overline{154},\ \bar{2}^{32} = \overline{154}^2 = \overline{640} = \overline{-1}.$$

34. (a) If $ax \equiv b$ has a solution x in $\mathbb{Z}_n$, then $b - ax = qn$, q an integer, so $b = ax + qn$. It follows that $d = \gcd(a, n)$ divides b. Conversely, if $d \mid b$ write $b = qd$, q an integer. Now $d = ra + sn$ for integers r and s (Theorem 3 §1.2), so $b = qd = (qr)a + (qs)n$. Thus, $(qr)a \equiv b (\text{mod}\, n)$ and we have our solution.

35. Working modulo p, $x^2 = \bar{1}$ means $x^2 - \bar{1} = \bar{0}$. Thus $(x - \bar{1})(x + \bar{1}) = \bar{0}$ in $\mathbb{Z}_p$, so $x = \bar{1}$ or $x = -\bar{1}$ by Theorem 7.

37. (a) If $n = p^2 m$ and $a = pm$, then $a \not\equiv 0 (\text{mod}\, n)$ and $a^2 \equiv 0 (\text{mod}\, n)$. Hence $a^n \not\equiv a$.

1.4 PERMUTATIONS

1. (a) $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}$ (c) $\tau^{-1} = \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$

(e) $\mu\tau\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix}$

3. (a) $\chi = \sigma^{-1}\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$ (c) $\chi = \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$

(e) $\chi = \tau^{-1}\varepsilon\sigma^{-1} = \tau^{-1}\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$

5. *Solution 1.* We must have $\sigma 1 = 1, 2, 3$ or 4; in each case we find $\sigma 1 = \sigma 3$, a contradiction.

If $\sigma 1 = 1:$

$$\begin{aligned} \tau 1 &= \tau\sigma 1 = 2 \\ \sigma 2 &= \sigma\tau 1 = 2 \\ \tau 2 &= \tau\sigma 2 = 3 \\ \sigma 3 &= \sigma\tau 2 = 1 \end{aligned}$$

If $\sigma 1 = 2:$

$$\begin{aligned} \tau 2 &= \tau\sigma 1 = 2 \\ \sigma 2 &= \sigma\tau 2 = 1 \\ \tau 1 &= \tau\sigma 2 = 3 \\ \sigma 3 &= \sigma\tau 1 = 2 \end{aligned}$$

If $\sigma 1 = 3:$

$$\begin{aligned} \tau 3 &= \tau\sigma 1 = 2 \\ \sigma 2 &= \tau\sigma 3 = 4 \\ \tau 4 &= \tau\sigma 2 = 3 \\ \sigma 3 &= \sigma\tau 4 = 3 \end{aligned}$$

If $\sigma 1 = 4:$

$$\begin{aligned} \tau 4 &= \tau\sigma 1 = 2 \\ \sigma 2 &= \sigma\tau 4 = 3 \\ \tau 3 &= \tau\sigma 2 = 3 \\ \sigma 3 &= \sigma\tau 3 = 4 \end{aligned}$$

Solution 2. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & d \end{pmatrix}$. Then we show $\sigma\tau = (a \quad b \quad c \quad d)$ is a cycle, contrary to $\sigma\tau = (1 \quad 2)(3 \quad 4):$

$$\begin{aligned} \sigma 1 = a &\Rightarrow \tau a = \tau\sigma 1 = 2 \Rightarrow \sigma\tau a = \sigma 2 = b \\ \sigma 2 = b &\Rightarrow \tau b = \tau\sigma 2 = 3 \Rightarrow \sigma\tau b = \sigma 3 = c \\ \sigma 3 = c &\Rightarrow \upsilon\tau c = \tau\sigma 3 = 4 \Rightarrow \sigma\tau c = \sigma 4 = d \\ \sigma 4 = d &\Rightarrow \tau d = \tau\sigma 4 = 1 \Rightarrow \sigma\tau d = \sigma 1 = a \end{aligned}$$

6. If $\sigma k = k$, then $\sigma^{-1}k = \sigma^{-1}(\sigma k) = k$. If also $\tau k = k$, then $(\tau\sigma)k = \tau(\sigma k) = \tau k = k$.

7. (a) Here $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & a & b & c & d \end{pmatrix}$ where a, b, c, d are 2, 3, 4, 5 in some order. Thus there are 4 choices for a, 3 for b, 2 for c, and 1 for d; and so we have $4 \cdot 3 \cdot 2 \cdot 1 = 4! = 24$ choices in all for σ.

(b) Now $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & a & b & c \end{pmatrix}$ where a, b, c are 3, 4, 5 in some order. As in (a), there are $3 \cdot 2 \cdot 1 = 3! = 6$ choices in all for σ.

8. (a) If $\sigma\tau = \varepsilon$, then $\sigma = \sigma\varepsilon = \sigma(\tau\tau^{-1}) = (\sigma\tau)\tau^{-1} = \tau^{-1}$.

9. If $\sigma = \tau$, then $\sigma\tau^{-1} = \tau\tau^{-1} = \varepsilon$; if $\sigma\tau^{-1} = \varepsilon$, then

$$\tau = \varepsilon\tau = (\sigma\tau^{-1})\tau = \sigma(\tau^{-1}\tau) = \sigma\varepsilon = \sigma.$$

11. (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 2 & 6 & 1 & 9 & 4 & 5 & 7 & 3 \end{pmatrix}$

12. (a) $\varepsilon, \sigma = (1 \quad 2 \quad 3)$, $\sigma^2 = (1 \quad 3 \quad 2)$, $\tau = (1 \quad 2)$, $\sigma\tau = (1 \quad 3)$, $\sigma^2\tau = (2 \quad 3)$. These are all six elements of S_3. We have $\sigma^3 = \sigma\sigma^2 = \varepsilon$, $\tau^2 = \varepsilon$ and hence $\tau\sigma = (2 \quad 3) = \sigma^2\tau$.

13. (a) $\sigma = (1\ 4\ 8\ 3\ 9\ 5\ 2\ 7\ 6)$; $\sigma^{-1} = (1\ 6\ 7\ 2\ 5\ 9\ 3\ 8\ 4)$
(c) $\sigma = (1\ 2\ 8)(3\ 6\ 7)(4\ 9\ 5)$; $\sigma^{-1} = (1\ 8\ 2)(3\ 7\ 6)(4\ 5\ 9)$
(e) $\sigma = (1\ 3\ 8\ 7\ 2\ 5)$; $\sigma^{-1} = (1\ 5\ 2\ 7\ 8\ 3)$

15. (a) $\varepsilon, (1\ 2\ 3\ 4\ 5),\ (1\ 2\ 3\ 4),\ (1\ 2\ 3),\ (1\ 2\ 3)(4\ 5),\ (1\ 2),\ (1\ 2)(3\ 4)$

17. (a) $\sigma^{-1} = (4\ 3\ 2\ 1)(7\ 6\ 5)$.

19. They are factored into disjoint cycles in the solution to Exercise 13, so the parities are:
(a) even (c) even + even + even = even (e) odd

21. (a) We have $\gamma_i^2 = \varepsilon$ for all i because the γ_i are transpositions. Hence $(\gamma_1\gamma_2 \dots \gamma_m)(\gamma_m\gamma_{m-1} \dots \gamma_2\gamma_2) = (\gamma_1\gamma_2 \dots \gamma_{m-1})(\gamma_{m-1} \dots \gamma_2\gamma_1) = \dots = \varepsilon$. Now use Exercise 8(a).

(c) If σ and τ are products of k and m transpositions respectively, then τ^{-1} is also a product of m transpositions (by (a)) so $\tau\sigma\tau^{-1}$ is a product of $k + 2m$ transpositions. This has the same parity as k.

23. Let $\sigma k = 1$ for some $k \neq 1$. Then, as $n \geq 3$, choose an $m \notin \{k, 1\}$. Now let $\gamma = (k, m)$. This gives $\gamma\sigma k = \gamma 1 = 1$, but $\sigma\gamma k = \sigma m \neq 1$, since if $\sigma m = 1 = \sigma k$, then $m = k$ as σ is one-to-one, contrary to assumption.

25. It suffices to show that any pair of transpositions is a product of 3-cycles. If k, l, m and n are distinct, this follows from

$$(k\ l)(m\ n) = (k\ m\ l)(k\ m\ n), (k\ l)(k\ m) = (k\ m\ l), \text{ and } (k\ l)^2 = \varepsilon.$$

27. (a) Both sides have the same effect on each k_i, and both sides fix each $k \notin \{k_1, k_2, \dots k_r\}$.

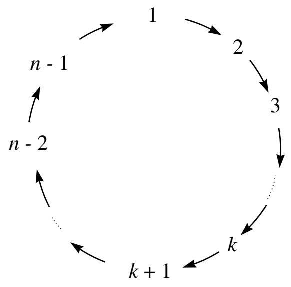
(c) Using Exercise 26, we have for all $a = 1, 2, \dots, n-1$:

$$(1\ a+1) = (1\ a)(a\ a+1)(1\ a) \qquad (*)$$

Now if $\sigma \in S_n$, write it as a product of factors $(1\ n)$. Use (*) to write each $(1\ n)$ as a product of $(1\ 2), \dots, (1\ n-1)$, and $(n-1\ n)$. Then write each $(1, n-1)$ in terms of $(1\ 2), \dots, (1\ n-2)$ and $(n-2, n-1)$. Continue. The result is (c).

28. (a) $\sigma = (1\ 2\ 3\ 4\ \dots\ 2k-1\ 2k)$ so $\sigma^2 = (1\ 3\ 5\ \dots\ 2k-1)(2\ 4\ 6\ \dots\ 2k)$.

(c) The action of σ is depicted in the diagram, and carries $k \to k+1 \to k+2 \dots$. If $k + m > n$, the correct location on the circle is given by the remainder r when $k + m$ is divided by n, That is $k + m \equiv 4(\mathrm{mod} n$. Now the action of σ^m is $\sigma^m k = k + m$, so $\sigma^m k \equiv k + m \bmod n$.



29. Each of σ and τ may be either even or odd, so four cases arise. They are the rows of the following table. The parity of $\sigma\tau$ in each case is clear, and so the result follows

σ	τ	$\sigma\tau$	sgn $\sigma\tau$	sgn σ	sgn τ
E	E	E	1	1	1
E	O	O	-1	1	-1
O	E	O	-1	-1	1
O	O	E	1	-1	-1

by verifying, sgn σ·sgnτ = sgn(τ) in every case.