(6) $100!$ 5^1 5^2

2^1 2^2 2^3 2^4 2^5 2^6

$2^1 5^1$ $2^2 5^1$ $2^3 5^1$ $2^4 5^1$ ~~$2^5 5^1$~~ ~~$2^6 5^1$~~

10 20 40 80

$5 \to 10 \to 15 \to 20 \to 25 \to 30 \to 35 \quad 40 \quad 45 \quad 50$

$4 \cdot 5^{+1}$ $\quad$ 2 $\quad$ 4 $\quad$ 2

$6 \cdot 4 = 24$ 5s in prime factorization

24 zeros

(11) 2^m+1 ~~odd~~ ~~prime~~ $\Rightarrow m = 2^n$

2	3	5	7	11	13	17
1	2	4	6	10	12	16

2^m+1

3	5	9	17	33	65	129	257
(1)	(2)	3	(4)	5	6	7	(8)

(10) $\log_2 3$ $2^p = 3^q$

Proof. Suppose $\log_2 3$ is rational. That is:

$\log_2 3 = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ $q \neq 0$

$2^{p/q} = 3$

$2^p = 3^q$

Contradiction. Let $n = 2^p$ $n \neq 3^q$ since there is only one way to write n as a product of primes.

(12) Proof. Consider the number $(n+1)! + 2$. We can list a consecutive integer sequence:

$(n+1)!+2, (n+1)!+3, (n+1)!+4, \ldots, (n+1)!+n+1$

Since $(n+1)! = (n+1)n(n-1)(n-2)\ldots(2)(1)$, $n+1 \mid (n+1)!$, $n \mid (n+1)!$, $\ldots, 2 \mid (n+1)!$. Since $n+1 \mid n+1$, $n \mid n, \ldots, 2 \mid 2$, we can conclude $n+1 \mid (n+1)!+n+1$, $n \mid (n+1)!+n, \ldots, 2 \mid (n+1)!+2$. We have found $(n+1)-2+1 = n$ consecutive composite integers.

(13) True. Let $p=3$. Then $p+2=5$, $p+4=7$. Since 3, 5, 7 are prime, there are three consecutive prime integers. ∴

(32) a) $\gcd(1,5) = \gcd(5 \bmod 1, 1) = \gcd(0,1) = 1$

e) $\gcd(1529, 14038) = \gcd(14038 \bmod 1529, 1529)$

$= \gcd(1529 \bmod 277, 277)$

$= \gcd(277 \bmod 144, 144)$

$= \gcd(144 \bmod 133, 133) = \gcd(133 \bmod 11, 11)$

$= \gcd(11 \bmod 1, 1)$

$= \gcd(0,1) = 1$

1529 | 14038 — 9 — 13761 — 277

277 | 1529 — 5 — 1385 — 144

277 − 144 = 133

(50) 6q Proof. Suppose $a, b, m \in \mathbb{Z}$ and $m \geq 2$ and $a \equiv b \pmod m$. So $a \bmod m = b \bmod m$. From the Euclidean algorithm,

$\gcd(a,m) = \gcd(a \bmod m, m) = \gcd(b \bmod m, m)$

$= \gcd(b, m)$

as desired.

(52) ~~Rob Pipe~~

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 211, 2311,

$p_1 p_2 \cdots p_n + 1 = kq + k - 1$

$p_1 p_2 \cdots p_n = k(q-1) + k - 1$

509 R 31 ; 531 ; 531 ; 6

Since 30031 is not prime, $p_1 p_2 \cdots p_n + 1$ is not always prime

210 × 11 = 2310; 2310 × 13 = 30030

2 → 6 → 30 → 210 → 2310 → 30030 → 510510 → 9699690 → 223092870

30030 × 17 = 210210 + 300300 = 510510

510510 × 19 = 9699690

9699690 × 23 = 194594 + 2185100 = 223092870

(53) ~~3k+4~~ 5k+4

7, 10, 13, 16, 19, 22

9, 14, 19, 24

3k+1

4, 7, 10, 13

5k+1

6, 11, 16, 21

k+1

2 3 (4)

k+1

240

Proof. Let $S_{a,b} = \{ak+b : k = 1, 2, \ldots \text{ and } a, b \in \mathbb{Z}_+\}$. Since $a(k+1)+b = ak+b+a$ Let $S'_{a,b} = \{ak+b+a : k = 1, 2, \ldots \text{ and } a, b \in \mathbb{Z}_+\}$ and $S'_{a,b} \subseteq S_{a,b}$. Observe that $b+a > 1$ so let $k = b+a$:

$ak+b+a \rightarrow a(b+a)+b+a = (a+1)(b+a)$

Since we can find a k that makes $ak+b+a$ composite, it follows that there is a composite number in $S'_{a,b}$ for any $a, b \in \mathbb{Z}_+$. But then $S_{a,b}$ also has a composite, as desired

(54) Suppose there are finitely many primes $q_1, q_2, \ldots, q_n$ of the form $3k+2$. Consider the number

$$3q_1q_2\ldots q_n - 1 = 3(q_1q_2\ldots q_n - 1) + 2$$

Since $3q_1q_2\ldots q_n - 1 > q_1, q_2, \ldots, q_n$ it is not prime. It is composite so there is a prime that divides $3q_1q_2\ldots q_n - 1$. Observe that $q_i \mid 3q_1q_2\ldots q_n$ for any $i \in \{1, 2, \ldots, n\}$. So $q_i \nmid 3q_1q_2\ldots q_n - 1$ since if otherwise, $q_i \mid 3q_1q_2\ldots q_n - (3q_1q_2\ldots q_n - 1)$ so $q_i \mid 1$ which is impossible. Since any prime of the form $3k+2$ doesn't divide the number, it must be in the form $3k+1$ or $3k$. But $3k$ is not prime unless $k=1$. Then we have a factor of 3 which is impossible. The proof is analogous to the $3k+2$ case. Observe that $3k+1 \bmod 3 = 1$ so

$$\left(\prod_{j=0}^{i}(3k_0+1)\right) \bmod 3 = 1$$

Meaning that any positive integer with prime factors of only the form $3k+1$ can be written according to the division algorithm as

$$\prod_{j=0}^{i}(3k_0+1) = 3\ell + 1 \qquad \ell \in \mathbb{Z}_+$$

But, $3q_1q_2\ldots q_n - 1 \bmod 3 \equiv -1 \pmod 3 \equiv 2 \pmod 3$. By the division algorithm,

$$3q_1q_2\ldots q_n - 1 = 3h + 2$$

But every number can be written uniquely in the division algorithm, so $3k+1$ is not a factor of $3q_1q_2\ldots q_n - 1$. Contradiction. There is a prime of form $3k+2 \notin \{q_1, q_2, \ldots, q_n\}$ as desired.

4.4 (6) a) $2 \bmod 17$

$17 = 2 \cdot 8 + 1$

$2 = 2 \cdot 1 = 17 - 2 \cdot 8$

$a^{-1} = -8$

(62) c) $144 \bmod 233$

$233 = 144 + 89$

$144 = 89 + 55$

$89 = 55 + 34$

$55 = 34 + 21$

$34 = 21 + 13$

$21 = 13 + 8$

$13 = 8 + 5$

$8 = 5 + 3$

$5 = 3 + 2$

$3 = 2 + 1$

$a^{-1} = 89$

$1 = 3 - 2$
$= 3 - 5 + 3$
$= 2(8-5) - 5$
$= 2(8) - 3(13-8)$
$= -3(13) + 5(21-13)$
$= 5(21) - 8(34-21)$
$= -8(34) + 13(55-34)$
$= 13(55) - 21(89-55)$
$= -21(89) + 34(144-89)$
$= -34(144) - 55(233-144)$
$= 89(144) - 55(233)$

(7) Suppose a and m are relatively prime in $\mathbb{Z}_+$. Suppose that b and c are solutions to $ax \equiv 1 \pmod{m}$. Then

$$ab \equiv ac \equiv 1 \pmod{m}$$
$$m \mid ab - ac$$
$$m \mid a(b-c)$$

By Euclid's lemma, and $m \nmid a$, $m \mid b-c$. So $b \equiv c \pmod{m}$ as desired.

(8) $\gcd(a,m) = as + mt > 1 \quad as \neq -mt$

$(as+mt) \bmod m = as \bmod m$

but $1 < as \bmod m < m$

Suppose $a \in \mathbb{Z}$, $m > 2$, and $\gcd(a,m) > 1$. We wish to prove the inverse of a modulo m does not exist. By Bézout's Theorem,

$$\gcd(a,m) = as + mt > 1 \quad \text{for some } s,t \in \mathbb{Z}$$

It follows that

$$(as+mb) \bmod m = as \bmod m$$
$$1 < as \bmod m < m$$

So $as \bmod m \neq 1 \bmod m$ and therefore $as \not\equiv 1 \pmod{m}$. We have shown that for any $s \in \mathbb{Z}$, s cannot be an inverse as desired.

(12) a) $34x \equiv 77 \pmod{89}$

~~$x \equiv 77 \cdot 08$~~

$34 \bmod 89$

$89 = 34 \cdot 2 + 21$

$34 = 21 + 13$

$21 = 13 + 8$

$13 = 8 + 5$

$8 = 5 + 3$

$5 = 3 + 2$

$3 = 2 + 1$

$1 = 3 - 2$

$= 3 - (5-3)$

$= -5 + 2(8-5)$

$= 2 \cdot 8 - 3(13-8)$

$= -3(13) + 5(21-13)$

$= 5(21) - 8(34-21)$

$= -8(34) + 13(89 - 34 \cdot 2)$

$= 13(89) - 34(34)$

$-34(34x) \equiv 77(-34) \pmod{89}$

$x \equiv -2618 \pmod{89}$

$x \equiv 52 \pmod{89}$

$\boxed{x = 52}$

$$\begin{array}{r} 2 \\ 77 \\ \times 34 \\ \hline 308 \\ 2310 \\ \hline 2618 \end{array}$$

$$\begin{array}{r} 29 \\ 89 \overline{)2618} \\ 178 \\ \hline 838 \\ 801 \\ \hline 37 \end{array}$$

$$\begin{array}{r} 89 \\ \times 30 \\ \hline 00 \\ 2670 \\ \hline 2670 \end{array}$$

$$\begin{array}{r} -2618 \\ \hline 52 \end{array}$$

b) $144x \equiv 4 \pmod{233}$ $\quad 144^{-1} = 89$

$89(144x) \equiv 4(89) \pmod{233}$

$x \equiv 356 \pmod{233}$

$\equiv 123 \pmod{233}$

$\begin{array}{r} 3 \\ 89 \\ \times\ 4 \\ \hline 356 \end{array}$ $\quad \boxed{x = 123}$

(16) a) $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$\{1, 6, 4, 3, 9, 2, 8, 7, 5\}$

2 mod 11

$2(6) \equiv 1 \pmod{11}$

$11 = 2 \cdot 5 + 1$

$2 = 1 + 1$

$1 = 2 - 1$

$1 = 3 \cdot 2 - 11$

3 mod 11

$11 = 3 \cdot 3 + 2$

$3 = 2 + 1$

$1 = 3 - 2$

$= 3 + 3 \cdot 3 + 11$

$= 4 \cdot 3 + 11$

$ab \equiv 1 \pmod{11}$

$cb \equiv 1 \pmod{11}$

$b(a - c) \equiv 0 \pmod{11}$

Proof. Let $A = \{2, 3, 4, \ldots, 8, 9\}$. Since $a \in A$ has property $\gcd(11, a) = 1$, by Bézout's Theorem, $11s + at = 1$ for $s, t \in \mathbb{Z}$ so t is the inverse of a. To show each $a \in A$ has a unique inverse, suppose b is the inverse of a_1 and a_2.

$a_1 b \equiv 1 \pmod{11}$

$a_2 b \equiv 1 \pmod{11}$

$a_1 b - a_2 b \equiv 0 \pmod{11}$

$b(a_1 - a_2) \equiv 0 \pmod{11}$

Since $11 \nmid b$, $11 \mid a_1 - a_2$. For some k, $11k = a_1 - a_2$ so $a_1 = 11k + a_2$. But $a \in A$ has $a < 11$ so $k = 0$ and $a_1 = a_2$. Therefore, the elements in A can be grouped with their inverses. This does not hold for 1 and 10 since they are their own inverses:

$1 \cdot 1 \equiv 1 \pmod{11}$

$10 \cdot 10 \equiv 1 \pmod{11}$

as desired.

(18) a) Proof. Let $A = \{2, 3, \ldots, p-1\}$. Since $a \in A$ has property $\gcd(a, p) = 1$, by Bezout's theorem, $at + ps = 1$ for $t, s \in \mathbb{Z}$. $at + ps \bmod p = 1$ so $at \bmod p = 1$. Therefore t inverse exists and is congruent to $a \in A$ modulo p since A is the set of all possible remainders except 0, 1 upon division by p. But $t \not\equiv 0 \pmod{p}$ since then $a(t^{-1}) \equiv 0 \pmod{p}$ and if $t \equiv 1 \pmod{p}$,

then t is the inverse of $q \in A$. Since $\gcd(q,p)=1$ then the inverse of $q \in A$ is unique. Since $|A| = p-3$, we have $(p-3)/2$ pairs of integers that are inverses of each other and lie between 1 and $p-1$.

b) Observe that for $A = \{2, 3, 4, \ldots, p-2\}$, the product of elements of A is $(p-2)!$. But the elements of A can be split into $(p-3)/2$ pairs (a_i, b_i) where $a_i, b_i \in A$ and $a_i b_i \equiv 1 \pmod{p}$. So:

$$a_1 b_1 \cdot a_2 b_2 \cdot \ldots \cdot a_i b_i \equiv 1 \pmod{p}$$
$$(p-2)! \equiv 1 \pmod{p}$$

Also, $p - 1 \equiv -1 \pmod{p}$ which can be verified:

$$p \mid p - 1 - (-1) \rightarrow p \mid p$$

So

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

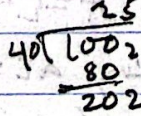
as desired.

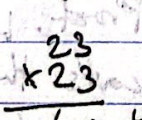
c) This means that $(p-2)! \not\equiv 1 \pmod{n}$, so the set $A = \{2, 3, \ldots, n-1\}$ cannot be split up into pairs of elements that are inverses of each other. It follows that for some $a \in A$, $\gcd(a, n) > 1$. Another case would be $n = 1$ or that $|A|$ is odd. All these imply that n is not prime.

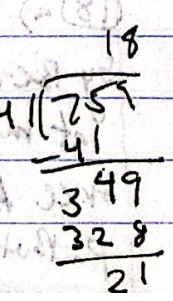
(34) Since $\gcd(23, 41) = 1$,

$$2^{40} \equiv 1 \pmod{41}$$
$$(2^{40})^{25} \cdot 23^2 \equiv 23^{1002} \pmod{41}$$
$$\equiv 23^2 \pmod{41}$$
$$\equiv 21 \pmod{41}$$

21







(4d) Let $n \in \mathbb{Z}_+$, Consider $n^7 - n$:

$$n^7 - n = n(n^6 - 1) = \cancel{n(n^3-1)(n^3+1) = n(}$$
$$= n(n^2-1)(n^4+n^2+1)$$
$$= n(n+1)(n-1)(n^4+n^2+1)$$

The important idea is that n^6-1, n^2-1, $n-1$ are factors of n^7-n. So consider the statements:

$$n^6 - 1 \equiv 0 \pmod 7 \quad (1)$$
$$n^2 - 1 \equiv 0 \pmod 3 \quad (2)$$
$$n - 1 \equiv 0 \pmod 2 \quad (3)$$

~~Two cases:~~ If $2|n$, we can cross out the statement (3) concerning modulo 2. If $3|n$, we can cross out (2) and the same idea if $7|n$. ~~Any~~ Combinations of these procedures allows us to represent any integer n with the corresponding correct statement. So if $2|n$, we have (1) and (2). Since n^2-1 and n^6-1 are factors of n^7-n, n^7-n is divisible by 3 and 7. But n is a factor of n^7-n so by $2|n$, 2 is also a factor. Thus $2 \cdot 3 \cdot 7$ is a factor. The proof is analogous to the other 6 7 cases.