

1. (a) The Euclidean algorithm produces the following steps:

$$13 = 8 + 5$$

$$8 = 5 + 3$$

$$5 = 3 + 2$$

$$3 = 2 + 1$$

so the greatest common divisor is 1. Working backwards yields

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) \\ &= 2(3) - 5 \\ &= 2(8 - 5) - 5 \\ &= 2(8) - 3(5) \\ &= 2(8) - 3(13 - 8) \\ &= 5(8) - 3(13) \end{aligned}$$

yielding the integer linear combination

$$1 = (-3)(13) + 5(8) .$$

- (b) The Euclidean algorithm produces the following steps:

$$27 = 21 + 6$$

$$21 = 3(6) + 3$$

so the greatest common divisor is 3. Working backwards yields

$$\begin{aligned} 3 &= 21 - 3(6) \\ &= 21 - 3(27 - 21) \\ &= 4(21) - 3(27) \end{aligned}$$

yielding the integer linear combination

$$3 = (-3)(27) + 4(21) .$$

(c) The Euclidean algorithm produces the following steps:

$$\begin{aligned}64 &= 2(25) + 14 \\25 &= 14 + 11 \\14 &= 11 + 3 \\11 &= 3(3) + 2 \\3 &= 2 + 1\end{aligned}$$

so the greatest common divisor is 1. Working backwards yields

$$\begin{aligned}1 &= 3 - 2 \\&= 3 - (11 - 3(3)) \\&= 4(3) - 11 \\&= 4(14 - 11) - 11 \\&= 4(14) - 5(11) \\&= 4(14) - 5(25 - 14) \\&= 9(14) - 5(25) \\&= 9(64 - 2(25)) - 5(25) \\&= 9(64) - 23(25)\end{aligned}$$

yielding the integer linear combination

$$1 = 9(64) + (-23)(25).$$

(d) The Euclidean algorithm produces the following steps:

$$\begin{aligned}2^{20} &= 2621(20^2) + 176 \\20^2 &= 2(176) + 48 \\176 &= 3(48) + 32 \\48 &= 32 + 16\end{aligned}$$

so the greatest common divisor is 16. Working backwards yields

$$\begin{aligned}16 &= 48 - 32 \\&= 48 - (176 - 3(48)) \\&= 4(48) - 176 \\&= 4(20^2 - 2(176)) - 176 \\&= 4(20^2) - 9(176) \\&= 4(20^2) - 9(2^{20} - 2621(20^2)) \\&= 23,593(20^2) - 9(2^{20})\end{aligned}$$

yielding the integer linear combination

$$1 = (-9)(2^{20}) + 23,593(20^2).$$

2. We sieve out all multiples of primes up to $\sqrt{100} = 10$, so remove all multiples of 2, 3, 5 and 7 leaving all primes less than 100:

2, 3, 5, 7, 11, 13, 17, 19, 23, 27, 29, 31, 37, 41, 43, 47, 53, 61, 67, 71, 73, 79, 83, 89, 97.

- *3. Certainly if N has a divisor M such that $1 < M \leq \sqrt{N}$ then $1 < M < N$ so that N is composite. Suppose on the other hand that N is composite. Then $N = ab$ for some integers a and b where $1 < a, b < N$. If $a > \sqrt{N}$ and $b > \sqrt{N}$ then

$$N = ab > (\sqrt{N})^2 = N,$$

which is impossible. Hence $a \leq \sqrt{N}$ or $b \leq \sqrt{N}$. This proves N has at least one nontrivial divisor $\leq \sqrt{N}$.

4. (a) $1,000,000 = 10^6 = (2 \times 5)^6 = 2^6 \cdot 5^6$.
 (b) $576,000 = 3 \times 192 \times 10^3 = 3 \times 32 \times 6 \times 2^3 \times 5^3 = 2^9 \cdot 3^2 \cdot 5^3$.
 (c) $100^2 - 98^2 = (100 + 98)(100 - 98) = 198 \times 2 = 99 \times 2^2 = 2^2 \cdot 3^2 \cdot 11^1$.

5. We calculate

$$\begin{aligned} 100^{100} &= 2^{100} \pmod{7} \\ &= (2^3)^{33} \times 2 \\ &= 1^{33} \times 2 \pmod{7} \\ &= 2, \end{aligned}$$

so that, after 100^{100} days have elapsed, it will be 2 days after a Monday, which is a Wednesday.

- *6. Observe first that

$$(-8)^2 = 64 = -8 \pmod{24}$$

from which it follows immediately that -8 coincides with all of its positive powers modulo 24. Thus

$$\begin{aligned} 100^{100} &= 4^{100} \pmod{24} \\ &= (4^2)^{50} \\ &= (-8)^{50} \pmod{24} \\ &= -8 \pmod{24} \\ &= 16 \pmod{24}, \end{aligned}$$

so that, after 100^{100} hours have elapsed, it will be 16 hours after some 9 a.m., which is 1 a.m. the following day. Thus $100^{100} - 16$ is a multiple of 24, so the number of days is

$$\frac{100^{100} - 16}{24} = \frac{2 - 2}{3} = 0 \pmod{7}.$$

Thus after $100^{100} - 16$ hours have elapsed it will again be 9 a.m. on a Monday, so that the meteor strike will be at 1 a.m. on the following Tuesday.

7. In \mathbb{Z}_7 we have

$$\frac{1}{2} = 4, \frac{1}{3} = 5, \frac{1}{4} = 2, \frac{3}{5} = 2, \frac{9}{10} = 3, \frac{10}{9} = 5.$$

In \mathbb{Z}_{11} we have

$$\frac{1}{2} = 6, \frac{1}{3} = 4, \frac{1}{4} = 3, \frac{3}{5} = 5, \frac{9}{10} = 2, \frac{10}{9} = 6.$$

In \mathbb{Z}_{10} , of these, only $\frac{1}{3} = 7$ and $\frac{10}{9} = 0$ exist.

*8. In \mathbb{Z}_{11} we have

$$\begin{aligned} & 1 + \frac{1}{2} + \cdots + \frac{1}{9} + \frac{1}{10} \\ &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{-5} + \frac{1}{-4} + \frac{1}{-3} + \frac{1}{-2} + \frac{1}{-1} \\ &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} - \frac{1}{5} - \frac{1}{4} - \frac{1}{3} - \frac{1}{2} - 1 \\ &= 0. \end{aligned}$$

Moreover, in \mathbb{Z}_p , where p is any odd prime, we have

$$\begin{aligned} & 1 + \frac{1}{2} + \cdots + \frac{1}{p-2} + \frac{1}{p-1} \\ &= 1 + \frac{1}{2} + \cdots + \frac{1}{(p-1)/2} + \frac{1}{-(p-1)/2} + \cdots + \frac{1}{-2} + \frac{1}{-1} \\ &= 1 + \frac{1}{2} + \cdots + \frac{1}{(p-1)/2} - \frac{1}{(p-1)/2} - \cdots - \frac{1}{2} - 1 \\ &= 0. \end{aligned}$$

9. (a) From the first question, $1 = (-3)(13) + 5(8)$, so that $8^{-1} = 5 \pmod{13}$.
 (b) Using the equation in (a) we get also that $13^{-1} = -3 = 5 \pmod{8}$.
 (c) From the first question, $1 = 9(64) + (-23)(25)$, so that $25^{-1} = -23 = 41 \pmod{64}$.
 (d) Since $\text{g.c.d.}(50, 64) = 2 \neq 1$, 50^{-1} does not exist in \mathbb{Z}_{64} .
10. (a) $3x = 5 \pmod{7}$ implies $x = 5/3 = 25 = 4 \pmod{7}$.
 (b) $37x = 52 \pmod{7}$ implies $2x = 3 \pmod{7}$, so that $x = 3/2 = 12 = 5 \pmod{7}$.
 (c) $7x = 6 \pmod{8}$ implies $x = 6/7 = 42 = 2 \pmod{8}$.
 (d) The equation $1 = 9(64) + (-23)(25)$ used in 9(c) gives $64^{-1} = 9 \pmod{25}$. Hence $64x = 3 \pmod{25}$ implies $x = 3/64 = 27 = 2 \pmod{25}$.

- *11.** We have $x = d_k d_{k-1} \dots d_2 d_1$ in base 10 where d_1, \dots, d_k are digits drawn from $0, \dots, 9$. Hence, using the fact that $10 \equiv 1 \pmod{9}$,

$$\begin{aligned} x &= d_1 + 10d_2 + 10^2d_3 + \dots + 10^{k-1}d_k \\ &\equiv d_1 + 1d_2 + 1d_3 + \dots + 1d_k \pmod{9} \\ &= d_1 + d_2 + d_3 + \dots + d_k. \end{aligned}$$

Since 9 is a multiple of 3 we have also that

$$x \equiv d_1 + d_2 + d_3 + \dots + d_k \pmod{3}.$$

Now, using the fact that $10 \equiv -1 \pmod{11}$, we get

$$\begin{aligned} x &= d_1 + 10d_2 + 10^2d_3 + \dots + 10^{k-1}d_k \\ &\equiv d_1 + (-1)d_2 + (-1)^2d_3 + \dots + (-1)^{k-1}d_k \pmod{11}. \end{aligned}$$

- **12.** Let N be any positive integer. Since there are infinitely many primes, choose a prime $p \geq N + 2$. List all the primes less than or equal to p :

$$p_1 < p_2 < \dots < p_M < p.$$

Note that $M \geq 1$. Put

$$Q = p_1 \times \dots \times p_M$$

and let

$$X = \{z \in \mathbb{Z} \mid Q + 2 \leq z \leq Q + p - 1\}.$$

Thus X consists of consecutive integers and has size $p - 2 \geq N$. Consider any $z \in X$. Then

$$2 \leq z - Q \leq p - 1 < p$$

so that $z - Q$ is a product of primes smaller than p . Hence p_i divides $z - Q$ for some $i \leq M$. But p_i also divides Q , so p_i divides $z - Q + Q = z$. This proves every element of X is composite.