Miscellaneous Number Theory Exercises

Matthew Gergley

Last Updated: January 31, 2026

Miscellaneous Exercises in Number Theory

Disclaimer: The proofs given are completed by myself. Thus, they are also reviewed by myself to ensure no logic flaws and incorrect arguments/deductions/conclusions. If you find any error in my proofs, please do not hesitate to contact me so we can discuss any potential errors and I can update the document as needed.

Contents

1 Miscellaneous

Exercise 1.1. Recall that the *The Sieve of Eratosthenes* can be used to check whether a number is prime.

(a) Prove *The Sieve of Eratosthenes* i.e., show that to check whether an integer $n > 1$ is prime, it suffices to divide by all primes $p \leq \sqrt{n}$. If n is not divisible by any of these, then n is prime.

(b) Use the Sieve of Eratosthenes to show that 173 is a prime number.

Proof. (a) Assume n is not prime. Hence $n = \prod\limits^{k} a_i$ for primes $a_i \leq n$. It follows that $a_i | n$ for all a_i. Also let all powers of each a_i s.t. n is completely factored. Assume $n = \prod\limits^{k} a_i$ is ordered such that $a_{k-1} \leq a_k$. Then $a_k < n$ since n has at least one other factor. If $a_k > \sqrt{n}$ then there exists some $(p < k) \in \mathbb{Z}$ s.t. a_p is the first time any a_i is less than a_k. So $a_p < a_k$ and it follows that $a_p \leq \sqrt{n}$. Thus $n = (\prod\limits^{p} a_i) \cdot a_k \Rightarrow (\prod\limits^{p} a_i) | n \Rightarrow a_p \cdot (\prod\limits^{p-1} a_i) | n \Rightarrow a_p | n$. Thus a_p is the closest prime less than or equal to $\sqrt{n}$ and it will detect that n is composite by checking only up to this prime a_p. If n was prime then it would not have a factorization and thus primes $p \nmid n$ for all $p < n$. Since it is prime you would only have to check if the primes $p \leq \sqrt{n}$ do not divide n which follows from the previous argument.

(b) We only need to check if the primes $p \leq \sqrt{173}$ divide 173. Thus we have to check primes $p \leq 13$.

$$\begin{aligned} 2 &\nmid 173 \\ 3 &\nmid 173 \\ 5 &\nmid 173 \\ 7 &\nmid 173 \\ 11 &\nmid 173 \\ 13 &\nmid 173 \end{aligned}$$

Therefore 173 is a prime.

□

Exercise 1.2. The Fibonacci Sequence is defined recursively in the following way:

$$f_0 = 0, \qquad f_1 = 1, \qquad f_n = f_{n-1} + f_{n-2} \text{ for } n = 2, 3, 4, \ldots$$

Using induction, show that

$$f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Proof. Base Case: $f_2 = f_1 + f_0 = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^1 - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^1 + \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^0 - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^0 = 1 + 0 = 1$ ✓ Assume $f_k = f_{k-1} + f_{k-2}$ for some integer $k \geq 2$. Thus WTS this is true for $k+1$. Then,

$$\begin{aligned} f_{k+1} &= f_k + f_{k-1} \\ &= \frac{(\frac{1+\sqrt{5}}{2})^k - (\frac{1-\sqrt{5}}{2})^k}{\sqrt{5}} + \frac{(\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^{k-1}}{\sqrt{5}} \end{aligned}$$

Grouping like terms, we get

$$\begin{aligned} &= \frac{1}{\sqrt{5}}\left[\frac{1+\sqrt{5}}{2})^k + \frac{(\frac{1+\sqrt{5}}{2})^k}{(\frac{1+\sqrt{5}}{2})}\right] - \left(\frac{1-\sqrt{5}}{2}\right)^k - \frac{(\frac{1-\sqrt{5}}{2})^k}{(\frac{1-\sqrt{5}}{2})} \\ &= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k\left(1 + \frac{2}{1+\frac{2}{1+\sqrt{5}}}\right)\right] - \left(\frac{1-\sqrt{5}}{2}\right)^k\left(1 + \frac{2}{1-\sqrt{5}}\right) \\ &= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k\left(\frac{3+\sqrt{5}}{1+\sqrt{5}}\right) - \left(\frac{1-\sqrt{5}}{2}\right)^k\left(\frac{3+\sqrt{5}}{1-\sqrt{5}}\right)\right] \end{aligned}$$

Then if we multiply $\frac{3+\sqrt{5}}{1+\sqrt{5}}$ and $\frac{3+\sqrt{5}}{1-\sqrt{5}}$ by $\frac{1-\sqrt{5}}{1-\sqrt{5}}$ and $\frac{1+\sqrt{5}}{1+\sqrt{5}}$ respectively, then

$$= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k\left(\frac{1+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)^k\left(\frac{1-\sqrt{5}}{2}\right)\right]$$

And thus we have

$$f_{k+1} = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k+1}$$

as desired.

□

Exercise 1.3. Prove that there are no integers between 0 and 1.

Proof. By way of contradiction, assume the set $S = \{x \in \mathbb{Z} \mid 0 < x < 1\} \neq \emptyset$. By the Well-Ordering Principle, we know that S has a smallest element x. Thus x exists such that it fulfills $0 < x < 1$ and $x \in \mathbb{Z}^+$. Now define $n = x^2$. Hence $n < x$ and $n \in \mathbb{Z}^+$ since $x \in \mathbb{Z}^+$ so $n > 0$. Then $n \in S$. But we said x was the least element of S and $n < x$. $\Rightarrow\Leftarrow$

□

Exercise 1.4. Show that every positive integer m has a unique binary expansion

$$m = \sum_{i=0}^{k} c_i 2^i = c_k 2^k + c_{k-1}2^{k-1} + \cdots + c_1 \cdot 2 + c_0$$

for some $k \in \mathbb{N}$ such that $c_k = 1$ and $c_i \in \{0, 1\}$ for $i = 0, 1, 2, \ldots, k-1$.

Proof. We can write $1 = 1 \cdot 2^0$. Therefore, assume that $n = \sum_{i=1}^{k} c_i 2^i$ for $1 \leq n \leq m$.
(Case 1: n is even)
By definition of n even, there exists some $l \in \mathbb{Z}$ s.t. $n = 2l$. But $l \leq n$ and thus by our induction hypothesis, $l = \sum_{i=1}^{k} c_i 2^i$. Thus $n = 2\sum_{i=1}^{k} c_i 2^i = \sum_{i=1}^{k} c_i 2^{i+1}$. We want to show that this is true for $n+1$ which will be enough to show that $n+1$ is odd since n is even. Thus
$n+1 = (\sum_{i=1}^{k} c_i 2^{i+1}) + 1 = 2(\sum_{i=1}^{k} c_i 2^i) + 1$ which is an odd number as desired.
(Case 2: n is odd)
Similarly, n being odd by definition means that there exists some $p \in \mathbb{Z}$ s.t. $n = 2p + 1$. But $p \leq n$ and thus by our induction hypothesis, $p = \sum_{i=1}^{k} c_i 2^i$. Then $n = 2(\sum_{i=1}^{k} c_i 2^i) + 1$. We want to show that this is true for $n+1$ again but this time $n+1$ should be an even number. Hence
$n+1 = (2(\sum_{i=1}^{k} c_i 2^i) + 1) + 1 = \sum_{i=1}^{k} c_i 2^{i+1} + 2 = 2((\sum_{i=1}^{k} c_i 2^i) + 1)$ which is even as desired.
Now to show that there are unique representations for any positive integer, assume there exist two binary representations for a number a. Thus $a = c_r 2^r + c_{r-1}2^{r-1} + \cdots + c_2 2^2 + c_1 2 + c_0$ and $a = c_s 2^s + c_{s-1}2^{s-1} + \cdots + c_2 2^2 + c_1 2 + c_0$ and assume that $r > s$ (the same argument could be made for $s > r$ as they are arbitrary). Then if we subtract these tow representations we should get 0. Hence,

$$c_r 2^r - c_s 2^s + c_{r-1}2^{r-1} - c_{s-1}2^{s-1} + c_{r-2}2^{r-2} - c_{s-2}2^{s-2} + \cdots$$

$$= 2^s(c_r 2^{r-s} - c_s) + 2^{s-1}(c_{r-1}2^{r-1-(s-1)} - c_{s-1}) + 2^{s-2}(c_{r-2}2^{r-2-(s-2)} - c_{s-2}) + \cdots$$

But since $r > s$ then $2^{s-i}(c_{r-i}2^{r-i-(s-i)} - c_{s-i})$ is always greater than 0 and thus this is a contradiction as the difference between the two representations is not 0 and thus $r = s$.

□

Exercise 1.5. Let G be a multiplicative group of order n. We will adopt the usual exponential notation. For example, $a^3 = a \cdot a \cdot a$. Then the group G is called *cyclic* if there exists an element $a \in G$ such that

$$G = \{a, a^2, a^3, \ldots, a^{n-1}, a^n\}. \tag{1}$$

(a) Show that the group U_{10} is a cyclic group.

(b) Show that the group U_{15} is not a cyclic group.

Proof. (a) Note that $U_{10} = \{1, 3, 7, 9\}$. We want to show that there exists an element $x \in U_{10}$ s.t. $|x| = \varphi(10) = 4$. The case of $x = 1$ does not satisfy $|x| = 4$ thus we will check 3. We get $3^1 \equiv 3,\ 3^2 \equiv 9,\ 3^3 \equiv 7,\ 3^4 \equiv 1$. Therefore $|3| = 4 = \varphi(10)$ and thus 3 is a cyclic generator of U_{10} s.t. $U_{10} = \langle 3 \rangle$, thus cyclic.

(b) Note that $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$. To show that U_{15} is not cyclic it is enough to show that for all $x \in U_{15}$, $|x| \neq \varphi(15) = \varphi(3 \cdot 5) = \varphi(3)\varphi(5) = 8$. The first case, when $x = 1$ trivially does not have order $\varphi(15)$ and thus we will check the remaining elements of U_{15}. Computing the orders of all the elements in U_{15}, except the trivial case, we find $|2| = 4, |4| = 2, |7| = 4, |8| = 4, |11| = 2, |13| = 4, |14| = 2$. Therefore since none of the elements have order $8 = \varphi(15)$, there doesn't exist a cyclic generator/primitive root in U_{15} and thus U_{15} is not cyclic.

□

Exercise 1.6. Show that multiplication is a closed binary operation on U_n, i.e., show that if $a \in U_n$ and $b \in U_n$, then $ab \in U_n$. Note: This completes the proof that U_n is a group.

Proof. Assume that $a, b \in U_n$ thus $\gcd(a, n) = \gcd(b, n) = 1$. BWOC assume that $ab \notin U_{29}$ hence $\gcd(ab, n) > 1$. Then there exists a prime p s.t. $p|ab$ and $p|n$. Therefore $p|a$ or $p|b$ but that means that either $\gcd(a, n) > 1$ or $\gcd(b, n) > 1$ which contradicts the assumption that $a, b \in U_n$. Therefore $\gcd(ab, n) = 1$ meaning $ab \in U_n$ and thus the multiplication is closed.

□

1.1 Fermat's Little Theorem Stuff

Exercise 1.7. Fermat's Little Theorem states that if p is prime and $\gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1 \mod p.$$

Prove this theorem by showing each of the following steps.

(a) Show that if $\gcd(a, p) = 1$ and p is prime, then the set

$$R = \{a, 2a, 3a, \dots, (p-1)a, pa\}$$

is a complete residue system modulo p, i.e., that R contains a representative of each equivalence class modulo p.

(b) Show that if p is prime and p does not divide a, then

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p$$

(c) Use Wilson's Theorem and (b) to show that

$$a^{p-1} \equiv 1 \mod p$$

Proof. (a) BWOC assume that there exists i, j where $1 \leq i, j \leq p$ and $i \not\equiv j$ s.t. $ia \equiv ja \mod p$. Then by the definition of congruence $p \big| ia - ja = a(i - j)$. Hence we have $p \big| a(i - j)$ and since p is prime then $p \big| a$ or $p \big| (i - j)$. But since $\gcd(a, p) = 1$, $p \nmid a$ so it must be the case that $p \big| i - j$. But $|i - j| < p$ therefore $p \nmid i - j$. This is a contradiction. Hence $ia \not\equiv ja$ for $i \not\equiv j$. Thus $a, 2a, 3a, \dots, pa$ are the representatives of p distinct congruence classes and thus form a complete residue system.

(b) Since $pa \equiv 0 \mod p$, via part (a) $a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p$.

(c) Lastly, by part (b) we have $a^{p-1}(p-1)! \equiv (p-1)! \mod p$. And by Wilson's Theorem $(p-1)! \equiv -1$. Hence $a^{p-1}(-1) \equiv -1 \mod p$. Multiplying by $-1^{-1} = -1$ on the right of both sides, we get $a^{p-1} \equiv 1 \mod p$.

□

Exercise 1.8. Use Fermat's Little Theorem to quickly calculate each of the following:

(a) $512^{372} \mod 13$

(b) $3444^{3233} \mod 17$

Proof. (a) To start, $512^{372} \mod 13$ can be rewritten via Fermat's Little Theorem and simplifying the base to obtain $(512 \mod 13)^{(372 \mod 13-1)}$. Thus,

$$\begin{aligned}(512 \mod 13)^{(372 \mod 13-1)} &\equiv 5^{31\cdot 12}\\ &\equiv (5^{12})^{31} \equiv (1)^{31} \equiv 1 \mod 13\end{aligned}$$

Observe that $5^{12} \equiv 1$ which follows directly from Fermat's Little Theorem of $a^{p-1} \equiv 1 \mod p$. Hence $512^{372} \equiv 1 \mod 13$.

(b) Via a similar process used in part (a), we can compute $3444^{3233} \mod 17$ using Fermat's Little Theorem. Thus simplifying the base and the exponent we obtain,

$$\begin{aligned}&(3444 \mod 17)^{(3233 \mod 17-1)} \equiv 10^{202\cdot 16+1}\\ &\equiv (10^{16})^{202} \cdot 16^{1} \equiv (1)^{202} \cdot 16 \equiv 16 \mod 17\end{aligned}$$

Again, observe the fact that $10^{16} \equiv 1$ which is a direct consequence of Fermat's Little Theorem and hence $3444^{3233} \equiv 16 \mod 17$.

□

Exercise 1.9. Use Fermat's Little Theorem to show that $7\big|11^{108} + 6$.

Proof. By definition, $7\big|11^{108} + 6$ means that $11^{108} \equiv -6 \mod 7$. Since $1 \equiv -6 \mod 7$ we have $11^{108} \equiv 1 \mod 7$. Simplifying the LHS, we get $(11 \mod 7)^{(108 \mod 7-1)}$. Thus $4^{6\cdot 18} \equiv (4^{6})^{18}$. By Fermat's Little Theorem, $4^{6} \equiv 1$ and thus we get $(1)^{18} \equiv 1 \mod 7$ which is simply $1 \equiv 1 \mod 7$ proving that $7\big|11^{108} + 6$.

□

Exercise 1.10. Find the inverse of $11 \mod 59$ using Fermat's Little Theorem and successive squaring. Then use it to find the unique solution to the congruence $11x \equiv 17 \mod 59$.

Proof. To start we wish to find 11^{-1} in $\mathbb{Z}_{59}$. Then $11^{-1} \equiv 11^{-1+(59-1)} \equiv 11^{57}$. Now we wish to compute 11^{57} using successive squaring. Thus,

$$\begin{aligned}&11^{2} \equiv 3 \mod 59\\ &11^{4} \equiv (11^{2})^{2} \equiv 3^{2} \equiv 9 \mod 59\\ &11^{8} \equiv (11^{4})^{2} \equiv 9^{2} \equiv 22 \mod 59\\ &11^{16} \equiv (11^{8})^{2} \equiv 22^{2} \equiv 12 \mod 59\\ &11^{32} \equiv (11^{16})^{2} \equiv 12^{2} \equiv 26 \mod 59\end{aligned}$$

Then we can write

$$\begin{aligned}&11^{57} \equiv 11^{32} \cdot 11^{16} \cdot 11^{8} \cdot 11\\ &\equiv 26 \cdot 12 \cdot 22 \cdot 11\\ &\equiv 75504 \equiv 43 \mod 59\end{aligned}$$

Therefore $11^{-1} \equiv 43$ in $\mathbb{Z}_{59}$. Now we can use this to find the solution to $11x \equiv 17 \mod 59$. Multiplying this linear congruence by 11^{-1} on the left we get $11^{-1} \cdot 11x \equiv 11^{-1} \cdot 17 \mod 59$. Since $11^{-1} \cdot 11 \equiv 1$ by definition, we get $x \equiv 43 \cdot 17 \equiv 731 \equiv 23 \mod 59$. Thus our solution is $x \equiv 23 \mod 59$.

□

2 Divisibility/GCD

Exercise 2.1. Use induction to show that $11^n - 6$ is divisible by 5 for every positive integer n.

Proof. $\underline{\text{Base case: } (n = 1)}$
$5 \mid 11^1 - 6 = 5 \mid 5$ ✓
Assume $5 \mid 11^k - 6 \; \forall \; k \in \mathbb{Z}^+$ meaning that $11^k - 6 = 5l$ for some integer l. WTS that this is true for $k + 1$ as well. Thus, $5 \mid 11^{k+1} - 6$. Manipulating the RHS we can write $11 \cdot 11^k - 6$. Furthermore, $11 \cdot 11^k - 66 + 60$ which we can then factor out 11 to get our induction hypothesis as so, $11(11^k - 6) + 60$. Thus substituting the hypothesis into this we get $11(5l) + 60$ which can be rewritten as $5(11l + 12)$. Thus we now have $5 \mid 5(11l + 12)$ in which the write hand side is a multiple of 5 since $11l + 12 \in \mathbb{Z}$ thus that statement is true and hence $5 \mid 11^n - 6$.

□

Exercise 2.2. Show that a positive integer d is the gcd of a and b if and only if

1) $d\big|a$ and $d\big|b$, and

2) if $e\big|a$ and $e\big|b$, then $e\big|d$.

Proof. ($\Rightarrow$) Assume that $d = \gcd(a, b)$ where $d \in \mathbb{Z}^+$. From the Euclidean Algorithm $d = r_{n-1}$. Also, $r_{n-2} = r_{n-1}q_n + r_n$ where $r_n = 0$. Thus by definition, $r_{n-1}|r_{n-2}$. And $r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}$ and since $r_{n-1}|r_{n-2}$, it follows that $r_{n-1}|r_i$ for $i = 1, 2, \dots$ which would lend to the fact that $r_{n-1}|a$ and $r_{n-1}|b$. But $r_{n-1} = d$ so $d|a$ and $d|b$. The last thing we wish to show is that if $e|a$ and $e|b$, then $e|d$. Hence, assume there exists an integer e s.t. $e|a$ and $e|b$. Again from the Euclidean Algorithm, $a = bq_1 + r_1$ which means that $r_1 = a - bq_1$. From our assumptions there exists $k, l \in \mathbb{Z}$ s.t. $r_1 = ek - elq_1 = e(k - lq_1)$ which by definition means $e|r_1$. Similarly, $r_2 = b - r_1q_2$ and thus substituting in r_1 and b we can get $r_2 = el - (e(k - lq_1))q_2 = e(l - q_2(k - lq_1))$ which implies that $e|r_2$. Continuing this argument we would find that $e|r_i$ for $i = 1, 2, \dots$. Then $e|r_{n-1}$. And recall $r_{n-1} = d$ so $e|d$ and thus $e \leq d$.
($\Leftarrow$) Assume that $d|a$ and and $d|b$, and if $e|a$ and $e|b$, then $e|d$. WTS that $d = \gcd(a, b)$. Clearly, d is common divisor of a and b. Now assume e is another common divisor of a and b. Then by our assumption, $e|d$. Hence $e \leq d$. Therefore, $d = \gcd(a, b)$.

□

Exercise 2.3. Let a and b be positive integers.

(a) Assume $\gcd(a, b) = 1$. Show that $\gcd(a + b, b) = 1$.

(b) Now assume $\gcd(a, b) = d \geq 1$. Show that

$$\gcd(a + b, b) = \gcd(a, b). \tag{2}$$

Proof. (a) BWOC assume there exists $a, b \in \mathbb{Z}^+$ s.t. $\gcd(a, b) = 1$ but $\gcd(a + b, b) \neq 1$. Thus, there exists $d \in \mathbb{Z}$ where $d > 1$ s.t. $\gcd(a + b, b) = d$. Then by definition, $d|a + b$ and $d|b$. Hence there exists $m, n \in \mathbb{Z}$ s.t. $a + b = dm$ and $b = dn$. In other words, $a = dm - b$ and $b = dn$. Then $a = dm - dn = d(m - n)$ which implies that $d|a$ and we also had $d|b$ but $d > 1$ and $\gcd(a, b) = 1$. This is a contradiction and thus $\gcd(a + b, b) = 1$ as well.

(b) Part (a) proves the case when $d = 1$ since we had $\gcd(a, b) = 1$ and $\gcd(a + b, b) = 1$ hence they are equivalent. Thus assume that $d > 1$. By definition, $\gcd(a, b) = d$ means that $d|a$ and $d|b$. Thus there exists $l, k \in \mathbb{Z}$ s.t. $a = dl$ and $b = dk$. BWOC, assume that $\gcd(a + b, b) \neq d$ i.e. $\gcd(a + b, b) = y$ for some integer $y \neq d$ and $y > 1$. Therefore, $y|a + b$ and $y|b$ by definition and thus there exists $m, n \in \mathbb{Z}$ s.t. $a + b = ym$ and $b = yn$. Thus rearranging the first equation and substituting in b we get $a = ym - yn = y(m - n)$ which implies that $y|a$. But $y \neq d$ when $\gcd(a, b) = d$. This contradiction leads to the fact that y must equal d. Thus $\gcd(a, b) = d = \gcd(a + b, b)$.

□

Exercise 2.4. Let a and b be relatively prime integers. Then

(a) If $a|c$ and $b|c$, then $ab|c$.

(b) If $a|bc$, then $a|c$.

Proof. (a) Assume $a\big|c$ and $b\big|c$. Thus there exists $l, k \in \mathbb{Z}$ s.t. $c = al$ and $c = bk$. Since $\gcd(a, b) = 1$, by Bezout's Identity there exists $x, y \in \mathbb{Z}$ s.t. $ax + by = 1$. Multiplying by c on both sides,

$$c = ax + cby = c,$$

substituting in what c is equal to from above,

$$(kb)ax + (la)by = c$$

$$ab(kx + ly) = c \;\Rightarrow\; ab|c.$$

(b) Assume $a\big|bc$. Thus there exists $l \in \mathbb{Z}$ s.t. $bc = la$. Since $\gcd(a, b) = 1$, by Bezout's Identity, there exists $ax + by = 1$. Multiplying both sides by c we obtain,

$$cax + cby = c.$$

Thus,

$$cax + (la)y = c,$$

by factoring, we obtain

$$a(cx + ly) = c \;\Rightarrow\; a|c.$$

□

Exercise 2.5. Prove the following Lemma and Corollary, which we used in the proof of the Fundamental Theorem of Arithmetic:

Lemma 2.1. If a prime p divides a product ab, then p divides at least one of a or b.

Corollary 2.1. If a prime p divides any finite product $m = a_1 a_2 \cdots a_k$, then $p\big|a_i$ for at least one i.

Proof. Lemma Proof: Assume $p|ab$. If $p\big|a$ we are done. Thus assume $p \nmid a$. By definition of $p\big|ab$, there exists $k \in \mathbb{Z}$ s.t. $ab = pk$. Since p is prime, $p \nmid a$ means that $\gcd(a, p) = 1$ hence there exists $x, y \in \mathbb{Z}$ s.t. $ax + py = 1$. Multiplying by b, $abx + pby = b$. Substituting ab in we obtain $pkx + pby = b$. Then $p(kx + by) = b$ and thus $p\big|b$.

Corollary Proof: Assume $p\big|m$ where $m = \prod_{i=1}^{k} a_i$. Then by the above lemma, either $p\big|a_1$ or $p\Big|\prod_{i=2} a_i$. If $p\big|a_1$ we are done, otherwise $p\Big|\prod_{i=2} a_i$. But by the lemma again, either $p\big|a_2$ or $p\Big|\prod_{i=3} a_i$. If $p\big|a_2$ we are done, otherwise apply the lemma to $p\Big|\prod_{i=3} a_i$ again. After at most k times there must be an integer $1 \leq l \leq k$ s.t. $p\big|a_l$ by the lemma.

□

Exercise 2.6. Assume n is a positive integer satisfying that whenever n divides a product ab, then $n\big|a$ or $n\big|b$. Show that n must be a prime number.

Proof. Assume n is composite and thus by definition $n = ab$ for $(a, b > 1) \in \mathbb{Z}$. Thus $n\big|ab$. But since $a, b < n$, $n \nmid a$ and $n \nmid b$. Hence the only time that $n\big|ab$ implies $n\big|a$ or $n\big|b$ is when n is prime.

□

Exercise 2.7. Prove that if n is a positive integer with k distinct odd prime factors, then 2^k divides $\varphi(n)$.

Proof. Let $n = p_1^{q_1} \cdot p_2^{q_2} \cdot p_3^{q_3} \cdots p_{k-1}^{q_{k-1}} \cdot p_k^{q_k}$ where the p_i's are odd primes and $q_i \in \mathbb{N}$. Then $\varphi(n) = \varphi(p_1^{q_1} \cdot p_2^{q_2} \cdot p_3^{q_3} \cdots p_{k-1}^{q_{k-1}} \cdot p_k^{q_k}) = \varphi(p_1^{q_1})\varphi(p_2^{q_2}) \cdots \varphi(p_k^{q_k}) = (p_1^{q_1} - p_1^{q_1-1})(p_2^{q_2} - p_2^{q_2-1}) \cdots (p_k^{q_k} - p_k^{q_k-1})$. Since p_i is prime for all $1 \leq i \leq k$, then p_i^r is odd for all $r \in \mathbb{N}$. Therefore every $p_i^{q_i}$ and $p_i^{q_i-1}$ are odd. Hence there exists integers l_j such that $\varphi(n) = ((2l_1+1) - (2l_2+1))((2l_3+1) - (2l_4+1)) \cdots ((2l_{2k-1}+1) - (2l_{2k}+1))$. Since p_i are unique primes, then every $2l_j + 1$ are unique distinct odd numbers. Then $((2l_1+1) - (2l_2+1))((2l_3+1) - (2l_4+1)) \cdots ((2l_{2k-1}+1) - (2l_{2k}+1)) = (2(l_1 - l_2)) \cdots (2(l_{2k-1} - l_{2k}))$. There are k many of these differences and multiples of 2, thus we obtain $\varphi(n) = 2^k((l_1 - l_2) \cdots (l_{2k-1} - l_{2k}))$ where $l_i - l_{i+1} > 0$. Then let $m = (l_1 - l_2) \cdots (l_{2k-1} - l_{2k})$ hence $m \in \mathbb{Z}^+$. Therefore $\varphi(n) = m \cdot 2^k \Rightarrow 2^k \mid \varphi(n)$.

□

3 Diophantine Equations

Exercise 3.1. Find the full set of integer solutions to the equation $49x + 21y = 7$.

Proof. Observe that $49x + 21y = 7$ is a Diophantine equation of the form $ax + by = c$ where $d = c = \gcd(a, b) = \gcd(21, 49) = 7$. Thus from the Euclidean Algorithm we can find the first solutions (x_0, y_0) and get $49 = 2 \cdot 21 + 7$ Hence $7 = 1 \cdot 49 + (-2) \cdot 21$ thus $(x_0, y_0) = (1, -2)$. In this case, our equation suffices $a, b \neq 0$ and $c = d = \gcd(a, b)$ with $(x_0, y_0) \in \mathbb{Z}^2$ is a solution to $ax + by = d$ results in the solution set of

$$S = \{(x_0 + \frac{b}{d}n, y_0 - \frac{a}{d}n) \colon n \in \mathbb{Z}\}.$$

The proof that this is in fact the solution set for this case is in the class notes. Thus the specific solution set for this Diophantine equation can be found by substituting our values,

$$S = \{(1 + 3n, -2 - 7n) \colon n \in \mathbb{Z}\}.$$

□

Exercise 3.2. Let a and b be nonzero integers, and let $d = \gcd(a, b)$. Assume that $d\big|c$, i.e., that $c = de$ for some integer e. Let (x_0, y_0) be any integer solution to the equation $ax + by = d$. Show that the complete set of integer solutions to the equation $ax + by = c$ is given by

$$S = \left\{ \left(x_0e + \frac{b}{d}n, y_0e - \frac{a}{d}n \right) \Big| \; n \in \mathbb{Z} \right\}.$$

Proof. First assume that (x_0, y_0) is a solution to $ax + by = c$. Then we have,

$$a\left(x_0e + \frac{b}{d}n\right) + b\left(y_0e - \frac{a}{d}n\right) = c$$

$$ax_0e + \frac{ab}{d}n + by_0e - \frac{ab}{d}n = c$$

$$ax_0e + by_0e = de$$

$$e(ax_0 + by_0) = de$$

Thus, $ax_0 + by_0 = d$ and since we assumed (x_0, y_0) was a solution then $(x_0e + \frac{b}{d}n, y_0e - \frac{a}{d}n)$ is a solution for all $n \in \mathbb{Z}$.

Now we want to show that all integer solutions are of this form. Assume we have two solutions, (x_0, y_0) and (x_1, y_1) s.t. $ax_0 + by_0 = d$ (1) and $ax_1 + by_1 = de$ (2). Thus if we subtract equation (1) and (2), we get $(1)y_1 - (2)y_0$ we would get $(ax_0 + by_0)y_1 - (ax_1 + by_1)y_0 = d(y_1 - y_0e)$. Rearranging the equation, we obtain $a(x_0y_1 - x_1y_0) = d(y_1 - y_0e)$. Likewise, we can do a similar subtraction of (1) minus (2) with the x_i, and obtain $(1)x_1 - (2)x_0$ and get $(ax_0 + by_0)x_1 - (ax_1 + by_1)x_0 = d(x_1 - x_0e)$. Again, rearranging this we can get, $b(x_1y_0 - x_0y_1) = d(x_1 - x_0e)$. Now let $n = x_1y_0 - x_0y_1$. Hence, $-an = d(y_1 - y_0e)$ and $bn = d(x_1 - x_0e)$. Now solving these equations for x_1 and y_1 we obtain

$x_1 = x_0e + \frac{b}{d}n$ and $y_1 = y_0e - \frac{a}{d}n$ and since (x_1, y_1) was an arbitrary integer solution, then every integer solution can be written in the form of the set $S = \left\{\left(x_0e + \frac{b}{d}n, y_0e - \frac{a}{d}n\right)\middle|\ n \in \mathbb{Z}\right\}$.

□

Exercise 3.3. List all pairs of integers (x, y) that satisfy the equation $49x + 21y = 63$.

Proof. Observe $\gcd(a, b) = \gcd(49, 21) = 7 = d$. Thus we can see that $c = 63$ so $d\big|c$. Hence there exists $e \in \mathbb{Z}$ s.t. $c = de$. Then $63 = 7e$ thus $e = 9$. To find our initial solution (x_0, y_0) we need (x, y) that satisfy $ax + by = d = 7$. Graphically, we can find that $(x_0, y_0) = (1, -2)$ is a solution to $49x + 21y = 7$. Thus to find the set of solutions we know it will be of the form

$$S = \left\{\left(x_0e + \frac{b}{d}n, y_0e - \frac{a}{d}n\right)\middle|\ n \in \mathbb{Z}\right\}$$

.

Thus substituting in our values, we get that the set of integer solutions to $49x + 21y = 63$ follows,

$$S = \left\{\left(9 + 3n, -18 - 7n\right)\middle|\ n \in \mathbb{Z}\right\}.$$

□

4 Pythagorean Triples

Exercise 4.1. Show that if (x, y, z) is a primitive Pythagorean triple, then x and y cannot both be even and cannot both be odd. *Hint: For the odd case, assume that there exists a primitive Pythagorean triple with x and y both odd. Then use Proposition 2.1.4 to produce a contradiction.*

Proof. Case 1: x, y even

By definition, a primitive triple is (x, y, z) that satisfy $x^2 + y^2 = z^2$ with $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$. BWOC assume there exists a primitive triple s.t. x, y are even. Hence there exists $m, n \in \mathbb{Z}$ s.t. $x = 2m$ and $y = 2n$. Thus $(2m)^2 + (2n)^2 = z^2$. So $2(2m^2 + 2n^2) = z^2$ which means that z^2 is even and thus z is even. But then $\gcd(x, y)$, $\gcd(x, z)$ and $\gcd(y, z)$ do **not** equal 1 since they share at least one factor of 2 since they are all even which contradicts the fact that x, y, z is a primitive triple.

Case 2: x, y is odd

BWOC assume there exists a primitive triple x, y, z where x, y are odd meaning there exists $m, n \in \mathbb{Z}$ s.t. $x = 2m + 1$ and $y = 2n + 1$. Then $(2m + 1)^2 + (2n + 1)^2 = 4m^2 + 4m + 1 + 4n^2 + 4n + 1 = z^2$. Hence, $z^2 = 4(m^2 + n^2 + m + n) + 2$. Let $k = m^2 + n^2 + m + n$, then $4k + 2 = z^2$. By proposition 2.1.4, $z^2 \mod 4 = 0$ or 1. If z is even, there exists $a \in \mathbb{Z}$ s.t. $z = 2a$ and thus $z^2 = 4a^2$. And if z is odd, then there exists $b \in \mathbb{Z}$ s.t. $z = 2b + 1$ and thus $z^2 = 4(b^2 + b) + 1$. Therefore if z is even, $z^2 \mod 4 = 0$ and if z is odd, $z^2 \mod 4 = 1$. But $4k + 2 \mod 4 = 2 \neq 0$ or 1. Thus, no primitive triple can have both x, y odd.

□

Exercise 4.2. Let $p = 8$ and $q = 13$. Generate the corresponding Pythagorean triple (see Theorem 3.4.5). Verify that indeed $x^2 + y^2 = z^2$ and that x, y, and z are pairwise relatively prime.

Proof. Observe $\gcd(p, q) = \gcd(8, 13) = 1$ and thus p, q are coprime. Then by Theorem 3.4.5, $z = p^2 + q^2 = (8)^2 + (13)^2 = 233$, $x = q^2 - p^2 = (13)^2 - (8)^2 = 105$, and $y = 2pq = 2(8)(13) = 208$. Furthermore, $x^2 + y^2 = (105)^2 + (208)^2 = 54289 = (233)^2 = z^2$. It also can be seen that $\gcd(105, 208) = \gcd(105, 233) = \gcd(208, 233) = 1$ and thus x, y, z are pairwise relatively prime.

□

5 Modular Arithmetic and Solving Congruence Relations

Exercise 5.1. Saying $a \equiv b \mod n$ is exactly the same as saying a and b leave the same remainder when divided by n

Proof. ($\Rightarrow$) Assume $a \equiv b \mod n$. Then by definition $n \big| a-b$ hence there exists $k \in \mathbb{Z}$ s.t. $a - b = nk$. Now write $a = nq_1 + r_1$ and $b = nq_2 + r_2$ by the division algorithm. Thus $nq_1 + r_1 - (nq_2 + r_2) = kn$. Then $r_1 - r_2 = kn - nq_1 + nq_2 = n(k - q_1 + q_2)$ which implies that $r_1 \equiv r_2 \mod n$. But we know by the division algorithm that $0 \leq r_i < b$ and r_i is $b \mod n$, thus $r_i < n$ thus if $r_1 \equiv r_2 \mod n$ it must be the case that $r_1 = r_2$. Hence they leave the same remainder when divided by n.
($\Leftarrow$) Assume a and b leave the same remainder when divided by n. Then, by the division algorithm, $a = nq_1 + r_1$ and $b = nq_2 + r_2$ for some $q_1, q_2, r \in \mathbb{Z}$. Then $a - b = n(q_1 - q_2)$. Therefore $n \big| a - b$ or in other words, $a \equiv b \mod n$.

□

Exercise 5.2. Use the properties of congruence and induction to show that if $a \equiv b \mod n$, then $a^m \equiv b^m \mod n$ for any positive integer m.

Proof. Assume $a \equiv b \mod n$. Then the case, $a^1 \equiv b^1 \mod n$ is clearly true. Thus, assume $a^k \equiv b^k \mod n$ is true for some $k \in \mathbb{Z}^+$. WTS that this is true for $k+1$ as well. From exercise 6, we know that if we have $a \equiv c \mod n$ and $b \equiv d \mod n$ then $ab \equiv cd \mod n$. Thus, from our assumptions, $a \equiv b \mod n$ and $a^k \equiv b^k \mod n$, then $a \cdot a^k \equiv b \cdot b^k \mod n$. Hence, $a^{k+1} \equiv b^{k+1} \mod n$.

□

Exercise 5.3. Prove that congruence is well-defined with respect to multiplication. That is, if $a \equiv c$ and $b \equiv d \mod n$, then $ab \equiv cd \mod n$.

Proof. Assume $a \equiv c \mod n$ and $b \equiv d \mod n$. Then by definition, there exists $k, l \in \mathbb{Z}$ s.t. $a - c = nk$ and $b - d = nl$. Hence $a = c + nk$ and $b = d + nl$. Thus,

$$ab = (c + nk)(d + nl)$$

$$= cd + cnl + dnk + n^2kl.$$

Thus $ab - cd = n(cl + dk + nkl)$. Let $m = cl + dk + nkl$, and thus $ab - cd = nm$ which implies that $ab \equiv cd \mod n$.

□

Exercise 5.4. Prove that 17 divides $291^7 + 8$ *without* the aid of a computing device that can do modular arithmetic (but definitely using congruence!).

Proof. Working in $\mathbb{Z}_{17}$,

$$\begin{aligned} 291^7 + 8 &\equiv 2^7 + 8 \\ &\equiv 2^4 \cdot 2^3 + 8 \quad \text{note in modulo 17, } 2^4 \equiv 16 \equiv -1 \\ &\equiv (-1) \cdot 2^3 + 8 \\ &\equiv 0 \pmod{17} \end{aligned}$$

Therefore, $17 | 291^7 + 8$.

□

Exercise 5.5. (a) Prove that the only solutions of $x^2 \equiv x \mod p$ are $x = [0]$ or $x = [1]$ if p is prime.

(b) Try to decide for *exactly* which composite moduli n the only solutions to $x^2 \equiv x \mod n$ are $x = [0]$ and $x = [1]$.

Proof. (a) Assume p is an odd prime. By definition $x^2 \equiv x \mod p$ means that $p \big| (x^2 - x) = x(x-1)$. By the lemma in Exercise 2, $p \big| x$ or $p \big| x - 1$. If $p \big| x$, then $x \equiv 0 \mod p$, else if $p \big| x - 1$, then $x - 1 \equiv 0 \mod p$ or in other words, $x \equiv 1 \mod p$. The case where $p = 2$, if $p \big| x$ then $p \big| x - 1$ since this would mean $x = 2k$ $(k \in \mathbb{Z})$ so $x - 1 = 2k - 1$ hence odd. Same argument can be made if $x - 1$ is even. Thus by the Lemma and the previous observations, you still would only obtain [0] and [1] as solutions.

(b) The only composites n that yield $x^2 \equiv x \mod n$ having solutions $x = [0], [1]$ are $n = 2^k$ $(k \geq 2) \in \mathbb{Z}^+$ since if $k = 1$ then $n = 2$ which is not composite. Hence $x^2 \equiv x \mod 2^k$ implies that $2^k \big| x^2 - x = x(x-1)$. Therefore by the above Lemma, either $2^k \big| x$ or $2^k \big| x - 1$. If $2^k \big| x$ then $x = 2l$ $(l \in \mathbb{Z})$ and thus $x \equiv 0 \mod 2^k$. Otherwise $2^k \big| x - 1$ and hence $x - 1 \equiv 0 \mod 2^k \Rightarrow x \equiv 0 \mod 2^k$. Then the only solutions for a composite modulus of the form $n = 2^k$ is $x = [0], [1]$ as desired.

□

Exercise 5.6. Find all solutions to the linear congruence $185x \equiv 475 \mod 715$ without the use of software that can do modular arithmetic.

Proof. Observe $715 = 5 \cdot 11 \cdot 13$. Thus we can write $185x \equiv 475 \mod 715$ as a system of three liner congruences.

$$\begin{aligned} 185x &\equiv 475 \mod 5 \\ 185x &\equiv 475 \mod 11 \\ 185x &\equiv 475 \mod 13 \end{aligned}$$

Reducing each expression by its modulus, we obtain,

$$\begin{aligned} &0x \equiv 0 \mod 5 \\ &9x \equiv 2 \mod 11 \\ &3x \equiv 7 \mod 13 \\ &\Downarrow \\ &0 \equiv 0 \mod 5 \\ &x \equiv 10 \mod 11 \\ &x \equiv 11 \mod 13 \end{aligned}$$

Therefore now we will apply the Chinese Remainder Theorem where $n = 715$, $n_1 = 5$, $n_2 = 11$, $n_3 = 13$, $N_i = \frac{n}{n_i}$ thus $N_1 = 143$, $N_2 = 65$, and $N_3 = 55$. Now we will write $N_i x_i \equiv 1 \mod n_i$ for $i = 1, 2, 3$.

$$\begin{array}{ccc} N_1x_1 \equiv 1 \mod 5 & N_2x_2 \equiv 1 \mod 11 & N_3x_3 \equiv 1 \mod 13 \\ 143x_1 \equiv 1 \mod 5 & 65x_2 \equiv 1 \mod 11 & 55x_3 \equiv 1 \mod 13 \\ 3x_1 \equiv 1 \mod 5 & 10x_2 \equiv 1 \mod 11 & 3x_3 \equiv 1 \mod 13 \\ x_1 \equiv 2 \mod 5 & x_2 \equiv 10 \mod 11 & x_3 \equiv 9 \mod 13 \end{array}$$

Now a solution to the original linear congruence can be found using $\bar{x} = \sum_{i=1}^{3} a_i N_i x_i$ where a_i are the RHS of the congruences above where we defined the Chinese Remainder Theorem values. Hence $\bar{x} = 0 \cdot 143 \cdot 2 + 10 \cdot 65 \cdot 10 + 11 \cdot 55 \cdot 9 \equiv 11945 \equiv 505 \mod 715$. Therefore all the solutions to $185x \equiv 475 \mod 715$ can be written as $505 + 715k$ $(k \in \mathbb{Z})$.

□

Exercise 5.7. Figure out how many solutions $x^2 \equiv x \mod n$ has for $n = 5, 6, 7$, and then compute how many solutions there are modulo 210.

Proof. We will compute how many solutions there are for each different modulus first through brute force. First $n = 5$. We have $0^2 \equiv 0 \mod 5$, $1^2 \equiv 1 \mod 5$, $2^2 \not\equiv 2 \mod 5$, $3^2 \not\equiv 3 \mod 5$, and $4^2 \not\equiv 4 \mod 5$. Thus for $n = 5$ we have 2 solutions. For $n = 6$, we will split it into two smaller n as $n - 6 = 2 \cdot 3$. Thus for $n = 2$ we both $0, 1$ being solutions thus we have 2 solutions. For $n = 3$ we also will have $0, 1$ being solutions and all to check is if 2 is a solutions but $2^2 \not\equiv 2 \mod 3$ and thus $n = 3$ also has 2 solutions. Lastly for $n = 7$ we will have $0, 1$ as solutions again, but have to check if there's any solutions from 2 to 6. Thus $2^2 \not\equiv 2 \mod 7$, $3^2 \not\equiv 3 \mod 7$, $4^2 \not\equiv 4 \mod 7$, $5^2 \not\equiv 5 \mod 7$, $6^2 \not\equiv 6 \mod 7$. Thus there is only two solutions for $n = 7$ as well. Thus the number of solutions for $n = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ is $2^4 = 16$ solutions.

□

Exercise 5.8. (a) Find all solutions to $x^2 + 8 \equiv 0 \mod 11$.

(b) Using your answer to part (a) and Hensel's Lemma, find all solutions to $x^2 + 8 \equiv 0 \mod 121$.

Proof.

(a) Checking all $k \in \mathbb{Z}_{11}$ as it is not too cumbersome, you will only find that $x_1 \equiv 5 \mod 11$ and $x_2 \equiv 6 \mod 11$ are solutions. More specifically, all solutions to $x^2 + 8 \equiv 0 \mod 11$ can be written as $5 + 11l$ and $6 + 11p$ for any $p, l \in \mathbb{Z}$.

(b) First we will solutions corresponding to $x_1 \equiv 5$. First note that $f'(x) = 2x$ and thus $\gcd(11, f'(5)) = \gcd(11, 10) = 1$. Now we can continue with Hensel's Lemma. We wish to solve for y in $f'(x_1)y \equiv -\frac{f(x_1)}{p^{e-1}} \mod 11$. Then $f'(5)y \equiv -\frac{33}{11} \mod 11$. We get $10y \equiv -3 \mod 11 \equiv 8 \mod 11$. Thus $10y \equiv 8 \mod 11$ results in $y \equiv 3$. Therefore $y_1 = x_1 + y \cdot p^{e-1} = 5 + 3 \cdot 11 = 38 \mod 121$. Now for $x_2 \equiv 6$ we check that $\gcd(11, f'(6)) = 1 = \gcd(11, 1)$ as desired. Thus we can use Hensel's Lemma. Again we wish to solve for y in the linear congruence $f'(6)y \equiv -\frac{44}{11} \equiv 7 \mod 11$. Thus since $f'(6) = 1$ we simply have that $y \equiv 7 \mod 11$. Therefore $y_2 = x_2 + y \cdot p^{e-1} = 83 \mod 121$. Therefore all solutions to $x^2 + 8 \equiv 0 \mod 121$ can be written as $y_1 = 38 + 121k$ or $y_2 = 83 + 121l$ for any $k, l \in \mathbb{Z}$.

□

Exercise 5.9. For which positive integers m is $26 \equiv 5 \mod m$?

Proof. By definition, $26 \equiv 5 \mod m$ means that $m \big| (26 - 5)$. This by definition further implies that there exists $k \in \mathbb{Z}$ s.t. $21 = mk$. Thus m can be the multiples of 21. Hence $m = 1, 3, 7,$ or 21.

□

Exercise 5.10. For which values of b does $bx^4 \equiv 2 \mod 29$ have at least one solution?

Proof. First we wish to obtain a primitive root in U_{29}. The primitive root will satisfy that if $x \in U_{29}$ is a primitive root, then $|x| = |U_{29}| = \varphi(29) = 28$. An element of U_{29} that satisfies this is 2 since $2^{\varphi(29)} \equiv 1 \mod 29$. Since we have identified this root, it is worth mentioning that there are $\varphi(\varphi(29)) = \varphi(28) = 12$ primitive roots including 2. Now we will write our congruence all in powers of our primitive root, 2. Let $b \equiv 2^y$ and $x \equiv 2^z$ for some $y, z \in U_{29}$. Hence we have,

$$\begin{aligned} 2^y(2^z)^4 &\equiv 2^1 \mod (29) \\ 2^{y+4z} &\equiv 2^1 \mod 29 \end{aligned}$$

Since both sides of the congruence have the same base 2, we wish to look at solutions to the exponents then which will be modulo 28. Thus,

$$\begin{aligned} y + 4z &\equiv 1 \mod 28 \\ 4z &\equiv 1 - y \mod 28 \end{aligned}$$

Here we can use the concept of finding a solution to a congruence $ax \equiv b \mod n$ and the fact that $d = \gcd(a, n)$ and $d|b$. So we have $\gcd(4, 28) = d = 4$ and thus $4|(1 - y)$. Essentially we are looking for y values that multiples of 4 plus 1. We find that $y \equiv 1, 5, 9, 13, 17, 21, 25$ satisfy this. Therefore the values of b that will yield at least one solution to this congruence are $b \equiv 2^1, 2^5, 2^9, 2^{13}, 2^{17}, 2^{21}, 2^{25} \equiv 2, 3, 19, 14, 21, 17, 11$.

□

5.1 Quadratic Congruences

Exercise 5.11. Solve the following quadratic congruence using the "completing the square" method:

$$9x^2 + 66x + 49 \equiv 0 \mod 79$$

Proof. Since $\gcd(2, 79) = \gcd(9, 79) = 1$, we know there exists 2^{-1} and 9^{-1} in $\mathbb{Z}_{79}$. Therefore we can use the completing the square method as follows,

$$\begin{aligned}9x^2+66x+49 \equiv 0 \pmod{79}\\ &\equiv 4(9^2x^2)+2\cdot 2\cdot 9\cdot 66x+66^2-66^2+4\cdot 9\cdot 49\\ &\equiv (18x)^2+4\cdot 9\cdot 66x+66^2\equiv 66^2-4\cdot 9\cdot 49\\ &\equiv (18x+66)^2\equiv 64 \pmod{79}.\end{aligned}$$

Thus, let $u=18x+66$, therefore $u^2\equiv 64$. The solutions to this simple quadratic congruence are $u\equiv -8\equiv 71 \mod 79$ and $u\equiv 8 \mod 79$. Now using these values, we can solve for the solutions x for $18x\equiv u-66 \mod 79$. We can compute $18^{-1}\equiv 18^{\varphi(79)-1}\equiv 22 \mod 79$. The first case is when $u=71$. We have $18x\equiv 71-66\equiv 5$. Multiplying by 18^{-1} on the left we obtain $x\equiv 22\cdot 5\equiv 31 \mod 79$. The second case is when $u=8$. Then we have $18x\equiv 8-66\equiv 21$. Multiplying by 18^{-1} on the left we obtain $x\equiv 22\cdot 21\equiv 67 \mod 79$. Hence the solutions to the quadratic congruence $9x^2+66x+49\equiv 0 \mod 79$ are $x\equiv 31$ and $x\equiv 67$.

□

5.2 Successive Squaring

Exercise 5.12. Compute $3^{87} \mod 7$ using the method of successive squaring and showing each step.

Proof.

$$\begin{aligned}3^2&\equiv 9\equiv 2 \pmod 7\\ 3^4&\equiv (3^2)^2\equiv 2^2\equiv 4 \pmod 7\\ 3^8&\equiv (3^4)^2\equiv (4)^2\equiv 16\equiv 2 \pmod 7\\ 3^{16}&\equiv (3^8)^2\equiv (2)^2\equiv 4 \pmod 7\\ 3^{32}&\equiv (3^{16})^2\equiv (4)^2\equiv 2 \pmod 7\\ 3^{64}&\equiv (3^{32})^2\equiv (2)^2\equiv 4 \pmod 7\end{aligned}$$

Therefore we can write,

$$\begin{aligned}3^{87}&\equiv 3^{64}\cdot 3^{16}\cdot 3^4\cdot 3^2\cdot 3 \pmod 7\\ &\equiv 4\cdot 4\cdot 4\cdot 2\cdot 3 \pmod 7\\ &\equiv (4)^2\cdot 4\cdot 6\equiv 2\cdot 4\cdot 6\equiv 48\equiv 6 \pmod 7\end{aligned}$$

□

Exercise 5.13. Compute $\varphi(1776)$ by hand. Then use Euler's theorem and successive squaring to find the unique solution equivalence class to the congruence

$$29x\equiv 119 \pmod{1776}$$

Proof. Let $n=1776$. Thus we can write n in its prime power factorization by $n=2^4\cdot 3\cdot 37$. Now we can compute $\varphi(1776)=\varphi(2^4\cdot 3\cdot 37)=\varphi(2^4)\varphi(3)\varphi(37)=(2^4-2^3)(3-1)(37-1)=576$. In our congruence $29x\equiv 119 \mod 1776$, $\gcd(29,1776)=1$ meaning there exits 29^{-1}. By Euler's theorem, $29^{-1}\equiv 29^{\varphi(1776)-1}\equiv 29^{575}$. Below we will use successive squaring to calculate this value.

$$
\begin{aligned}
29^2 &\equiv 841\\
29^4 &\equiv 433\\
29^8 &\equiv 1009\\
29^{16} &\equiv 433\\
29^{32} &\equiv 1009\\
29^{64} &\equiv 433\\
29^{128} &\equiv 1009\\
29^{256} &\equiv 433\\
29^{512} &\equiv 1009\\
29^{575} &\equiv 29^{512} \cdot 29^{32} \cdot 29^{16} \cdot 29^{8} \cdot 29^{4} \cdot 29^{2} \cdot 29\\
&\equiv 245 \mod 1776
\end{aligned}
$$

Therefore $29^{-1} \equiv 245 \mod 1776$. Multiplying $29x \equiv 119 \mod 1776$ by 29^{-1} on the left on both sides, we get $x \equiv 29^{-1} \cdot 119 \equiv 245 \cdot 119 \equiv 739 \mod 1776$. Thus $x \equiv 739 \mod 1776$.

□

6 CRYPTOGRAPHY!!!

Exercise 6.1. Encode the message

CRYPTOGRAPHYISFUN

using the following letter assignment: $a \to 0, \quad b \to 1, \quad c \to 2,$ etc. Then encrypt the message using the shift cipher key $k \equiv 16 \mod 26$.

Proof. First we must apply the letter assignment to CRYPTOGRAPHYISFUN. Following the fact that $a \to 0, \quad b \to 1, \ldots$, we obtain $x = 2, 17, 24, 15, 19, 14, 6, 17, 0, 15, 7, 24, 8, 18, 5, 20, 13$. Now we have to apply to shift of $k \equiv 16 \mod 26$. Thus we will calculate $m_i \equiv x_i + k \mod 26$ for all x_i where m_i is x_i encrypted with the shift cipher and m is our entire encrypted message. Thus we get,

$$
\begin{aligned}
m &\equiv (2+16), (17+16), (24+16), \ldots, (20+16), (13+16) \mod 26\\
&\equiv 18, 7, 14, 5, 9, 4, 22, 7, 16, 5, 23, 14, 24, 8, 21, 10, 3 \mod 26
\end{aligned}
$$

□

Exercise 6.2. Help Eve evesdrop on a conversation between Alice and Bob.

(a) Eve intercepts the following messages between Alice and Bob:

1. (A → B) $g = 17$, $p = 31$
2. (A → B) 12
3. (B → A) 24

She knows that Alice and Bob are exchanging a shift cipher key using Diffie-Hellman key exchange. Help Eve find the key $k \mod 31$.

(b) After finding the shift cipher key, Eve intercepts the following message from Alice to Bob:

21, 23, 20, 18, 20, 11, 21, 7, 18, 3, 20, 22, 1, 8, 17, 20, 7, 24, 7, 3, 22, 21, 11, 0, 18, 15

Help Eve decrypt this message.

Proof. (a) Given this information, we need to find a or b which are numbers that Alice and Bob choose. Therefore, we need to solve either $g^a \equiv x \mod 31$ or $g^b \equiv y \mod 31$ for a or b. Simultaneously we will solve both of these just to confirm the fact that having either a or b will give us the same key k. So the two congruences we have are $17^a \equiv 12 \mod 31$ and $17^b \equiv 24 \mod 31$. Using Python, we can brute force this since the numbers are small as well as the modulus of 31 and we find that $a \equiv 7$ and $b \equiv 19$ satisfy these congruences. Thus to find the key all we must compute is $k \equiv (g^a)^b \equiv (g^b)^a \equiv g^{ab} \equiv 17^{7 \cdot 19} \equiv 3 \mod 31$. Thus the key is $k \equiv 3 \mod 31$.

```

        p = 31
        g = 17
        for i in range(1,p):
            if (g**i)%p == 12 or (g**i)%p == 24:
                print('i',i,'g^i=',(g**i)%p)

```

Listing 1: Calculating a and b

(b) We are given a message $m \equiv x + k \mod 31$ so to decrypt this message, since we know it is shifted by k, all we need to do it subtract k from every encrypted letter. Formally, $x \equiv m - k$ where x is the decrypted message. Note this operation is performed on every encrypted letter. Utilizing Python to do this we obtain, the following message:

surprisepartyforeveatsixpm

```

        p = 26
        k = 3
        lst1 = [21, 23, 20, 18, 20, 11, 21, 7, 18, 3, 20, 22, 1, 8, 17,
                20, 7, 24, 7, 3, 22, 21, 11, 0, 18, 15]
        string1 = ""

        dic1 = {0:'a',1:'b',2:'c',3:'d',4:'e',5:'f',6:'g',7:'h',8:'i',
                9:'j',10:'k',11:'l',12:'m',13:'n',14:'o',15:'p',16:'q',
17:'r',18:'s',19:'t',20:'u',21:'v',22:'w',23:'x',24:'y',
                25:'z'}

        for num in lst1:
            string1 += dic1[(num-k)%p]
        print(string1)

```

Listing 2: Shifting the letters by k

□

Exercise 6.3. 1. Is the number 1425379893 a valid ISBN? Justify your answer.

2. The number 2841456784 is obtained from a valid ISBN number by switching two consecutive digits. Find the ISBN number.

3. Find an example of a single invalid 10-digit number that can be obtained from two distinct valid ISBN numbers, where each valid ISBN is obtained from the invalid number via a single swap of two consecutive digits. List the invalid number and the two corresponding valid ISBN numbers.

Proof. (a)

$$\begin{aligned} x_{10} &\equiv \sum_{i=1}^{9} i \cdot x_i \mod 11 \\ &\equiv (1)(1) + (2)(4) + (3)(2) + (4)(5) + (5)(3) + (6)(7) \\ &\quad + (7)(9) + (8)(8) + (9)(9) \\ &\equiv 300 \equiv 3 \mod 11. \end{aligned}$$

Thus since the calculated check digit, $x_10 \equiv 3 \mod 11$, and 3 is the last digit of the ISBN 1425379893 thus it is a valid ISBN.

(b) First we want to check if 2841456784 is a valid ISBN. Applying the same logic as part (a), we expect to get $x_{10} \equiv 4$.

$$\begin{aligned} x_{10} &\equiv \sum_{i=1}^{9} i \cdot x_i \mod 11 \\ &\equiv (1)(2) + (2)(8) + (3)(4) + (4)(1) + (5)(4) + (6)(5) \\ &\quad + (7)(6) + (8)(7) + (9)(8) \\ &\equiv 254 \equiv 1 \not\equiv 4 \mod 11. \end{aligned}$$

Thus, this is not a valid ISBN number and we have to check to see which digits were swapped due to a potential error typing. The way to do this is to test swapping consecutive digits and calculating this sum and taking modulo 11 is congruent to 4 (the check digit). Hence, the Python program below will do just that:

```python

        def calculate_check_digit(isbn):
            total = sum(int(digit) * (index + 1) for index, digit in enumerate(isbn[:-1]))
            return total % 11

        def swap_consecutive_digits(isbn):
            check_digit = calculate_check_digit(isbn)
            last_digit = int(isbn[-1])

            if check_digit == last_digit:
                return isbn

            for i in range(len(isbn) - 1):
                if i == 0:
                    swapped_isbn = isbn[1] + isbn[0] + isbn[2:]
                else:
                    swapped_isbn = isbn[:i] + isbn[i + 1] + isbn[i] + isbn[i + 2:]

                if calculate_check_digit(swapped_isbn) == last_digit:
                    return swapped_isbn

            return None

        invalid_isbn = "2841456784"
        corrected_isbn = swap_consecutive_digits(invalid_isbn)
        if corrected_isbn:
            print("Corrected ISBN:", corrected_isbn)
        else:
            print("No pair of consecutive digits can be swapped to achieve the desired result.")


```

Listing 3: Detecting Digit Swap in ISBN 10

The output of the code when testing our invalid ISBN, 2841456784, is "Corrected ISBN: 2814456784". Hence the third and fourth digit, 4 and 1 respectively, were swapped creating an invalid ISBN. Thus the valid ISBN number is 2814456784.

(c) The idea behind this derivation is that we want to construct an ISBN number where there is two distinct pairs of consecutive digits that have the same difference between them. For our case we will consider $(x_1 - x_2) = (x_3 - x_4)$. Thus we can have 758631924. Note that there are at least two instances of consecutive digits have the same difference but namely the prior equation follows for this number, $(x_1 - x_2) = (x_3 - x_4)$. The check digit for this number can be calculated by,

$$x_{10} \equiv \sum_{i=1}^{9} i \cdot x_i \mod 11,$$

which gives you that $x_{10} \equiv 3 \mod 11$. But if we swap x_1 and x_2, we get the ISBN number 578631924 with a check digit of $x_{10} \equiv 5 \mod 11$ and if we also swap x_3 and x_4 in the original ISBN we get 756831924 with a check digit also of $x_{10} \equiv 5 \mod 11$. Thus our invalid ISBN number will be the original ISBN with 5 as its check digit since we know that its check digit is actually supposed to be 3. Therefore,

Incorrect ISBN: 7586319245
Valid ISBN's: 5786319245 and 7568319245

□

Exercise 6.4. 1. Write a detailed explanation of how the 13-digit ISBN check digit is computed.

2. Show that ISBN 13 always detects a single transcription error (a single digit is typed incorrectly).

3. Does ISBN 13 always detect a swap error like ISBN 10 does? Justify your answer.

Proof. (a) The process to calculate the check digit of a 13-digit long ISBN is quite different than a 10 digit ISBN. Suppose we have a 13-digit long ISBN, the check digit is calculated by multiplying the first number in the ISBN by 1 and then adding it to the second number of the ISBN multiplied by 3 then that is added to the third number of the ISBN multiplied by 1 and this pattern follows all the way up to the 12th digit which is added to the continuous summation by multiplying the 12th digit by 3 and adding it into the sum. In other words, if we index the ISBN number from 1 to 12, if the number's index is odd then we multiply it by 1 and if the index is even then we multiply by 3. Then, once we get that sum, we take the sum modulo 10 and if the resulting remainder is 0 then the check digit is 0, and if it is not 0 then the check digit is 10 minus the remainder after taking the sum modulo 10. Mathematically,

$$x_{13} \equiv \left[10 - (\sum_{i=1}^{12}(2+(-1)^i)x_i \mod 10)\right] \mod 10$$
$$\text{if } x_{13} \equiv 0, \text{ then the check digit is } 0$$
$$\text{otherwise the check digit is } 10 - x_{13}$$

(b) Assume x_{13} is the valid check digit to an ISBN 13. Then $\sum_{i=1}^{13}(2+(-1)^i)y_i \mod 10 \equiv 0$. Now assume that a transcription error has occurred thus $y_j \neq x_j$ for one value of j. If a transcription error occurred then $y_{13} \not\equiv \sum_{i=1}^{12}(2+(-1)^i)y_i \mod 10$. Adding $1 \cdot x_{13}$ to both sides of the congruence gives us

$$\sum_{i=1}^{12}(2+(-1)^i)x_i \equiv x_{13} \mod 10$$
$$\Rightarrow \sum_{i=1}^{13}(2+(-1)^i)x_i \equiv 0 \mod 10$$

Then,

$$\sum_{i=1}^{13}(2+(-1)^i)y_i \equiv \sum_{i=1}^{13}(2+(-1)^i)y_i - \sum_{i=1}^{13}(2+(-1)^i)x_i$$
$$= j(y_j - x_j)$$

If the transcription error occurred at an even index, j is even, then $3(y_j - x_j) \not\equiv 0 \mod 10$ because we know that $1 \leq y_j - x_j \leq 9$ and therefore the only value that would be congruent to 0 mod 10 when multiplied by 3 is if $y_j - x_j = 10$ which is not possible. Now if j is odd, then $1(y_j - x_j) \not\equiv 0 \mod 10$ since again $1 \leq y_j - x_j \leq 9$. Thus a transcription error of a single digit will always be detected.

(c) ISBN 10 is able to detect transpositions whether it is between two adjacent positions or beyond that. However, ISBN 13 is only able to detect transpositions of adjacent numbers. Suppose we have an ISBN 13 number defined as $x_1x_2x_3\cdots x_{12}x_{13}$. If we transposed x_2 with x_6, then we would end up with,

$$\sum_{i=1}^{k}(2+(-1)^k)x_i$$

$$= 1\cdot x_1 + 3\cdot x_6 + 1\cdot x_3 + \cdots + 3\cdot x_2 + 1\cdot x_7 + \cdots$$

Thus it follows that if you swap numbers with the parity in the index, it would be unrecognizable since you would be multiplying x_i by either 1 or 3 no matter what just in a different order which doesn't matter since addition is commutative. But if you switch digits that are opposite parity in their indices, you will be able to detect a swap error due to the fact that you would have an expression similar to (b) but including the fact that there two indices involved you get $10\big|(k-j)(y_k-y_j)$ where $k > j$ and $k-j$ will always be 2 and thus as long as the difference between $y_k - y_j$ is not a multiple of 10 which is only true if $(y_k - y_j) = 5$. Below is a python algorithm that will compute take a valid ISBN and detect an invalid ISBN from a swap of digits:

```python
import random as r

def isbn_checkDigit(num):
    xsum = 0
    num = str(num)
    for i in range(1, 13):
        if i % 2 == 0:
            xsum += 3*int(num[i-1])
        else:
            xsum += int(num[i-1])
    return (10 - (xsum % 10)) % 10

def findSwapError(num):
    num = str(num)
    check = isbn_checkDigit(num)

    for i in range(len(num)-1):
        if i == 0:
            swappedIsbn = num[1] + num[0] + num[2:]
        else:
            swappedIsbn = num[:i] + num[i+1] + num[i] + num[i+2:]
        if isbn_checkDigit(str(swappedIsbn)) != check:
            return swappedIsbn
    return False

found_swap_error = False
while not found_swap_error:
    testnum = ""
    for i in range(1, 13):
        testnum += str(r.randint(1, 9))
    found_swap_error = findSwapError(int(testnum))
    if found_swap_error:
        print(f"Original ISBN: {testnum} with check digit {isbn_checkDigit(testnum)}. Swapped ISBN: {found_swap_error} "
              f"with check digit {isbn_checkDigit(found_swap_error)}")

```

Listing 4: Detecting Digit Swap in ISBN 13

□

Exercise 6.5. The following message was sent by Bob to Alice:

QLGDOABYNPGCBMNJY

Eve knows that Bob used an affine cipher with $n = 26$ and the usual encoding:

$$\text{A} \mapsto 0,\ \text{B} \mapsto 1,\ \text{C} \mapsto 2, \ldots$$

Help Eve break this cryptosystem and recover Bob's secret message to Alice. *Hint: Brute force using a computer is likely to be the best option here.*

Proof. We know that a affine cipher is the general case of a shift cipher. If we have the original message x, we first assign each letter to numbers and then multiply it by a key a and then add b to it. This gives us the encrypted message y. Formally, $y = ax + b$. However, we don't know a or b so we have to brute force by the fact that $1 \leq a \leq 25$ and $1 \leq b \leq 25$. Using Python, we find that $a = 7$ ad $b = 12$ gives us a message with meaning in English. The message states, "I LOVE CRYPTOGRAPHY".

```
def mod_inv(a, m):
    for x in range(1, m):
        if (a * x) % m == 1:
            return x
    return None

def affine_decrypt(ciphertext):
    plaintext = ''
    m = 26
    for a in range(1, m):
        a_inv = mod_inv(a, m)
        if a_inv is None:
            continue
        for b in range(m):
            decrypted_text = ''
            for char in ciphertext:
                if char.isalpha():
                    char_num = ord(char) - ord('A')
                    decrypted_num = (a_inv * (char_num - b)) % m
                    decrypted_text += chr(decrypted_num + ord('A'))
                else:
                    decrypted_text += char
            print(f"a={a}, b={b}: {decrypted_text}")

print(affine_decrypt('QLGDOABYNPGCBMNJY'))

```

Listing 5: functions to break cipher brute force

□

Exercise 6.6. Alice and Bob are using Diffie-Hellman key exchange to agree on a private shift cipher key. Alice chooses the prime number $p = 29$ and the modular number $g = 7$ and sends these to Bob. Bob chooses the exponent $b = 5$, and Alice chooses the exponent $a = 11$.

(a) What is the next modular number that Alice sends to Bob?

(b) What is the next modular number that Bob sends to Alice?

(c) What is the private shift cipher key that they compute?

(d) Use the shift cipher key obtained in part (c) to encrypt the following message from Bob to Alice: HIALICE

Proof. (a) The next modular number that Alice will send to Bob is of the form $g^a \mod p$. Thus she sends $7^{11} \equiv 23 \mod 29$.

(b) The modular number that Bob will send to Alice is of the form $g^b \mod p$. Thus he sends $7^5 \equiv 16 \mod 29$.

(c) Both Alice and Bob will compute the private shift cipher key by raising the modular number they receive from each other by their respective chosen exponent following $\gcd(a, p-1) = \gcd(b, p-1) = 1$. Formally, they would compute either $(g^b)^a$ or $(g^a)^b$ and reduce modulo p. Thus, the private shift cipher key is $k \equiv (16)^{11} \equiv 25 \mod 29$.

(d) Using the usual encoding of $a \mapsto 0, b \mapsto 1, \ldots$, we can encode HIALICE into $7, 8, 0, 11, 8, 2, 4$. Now we add $k \equiv 25$ to all of these encoded values and reduce modulo 26 since we are using a 26 letter alphabet. Thus we obtain the encrypted message as $6, 7, 25, 10, 7, 1, 3$ which if we apply the letter assignment based off of our alphabet above we have GHZKHBD.

```
dic1 = {0:'a',1:'b',2:'c',3:'d',4:'e',5:'f',6:'g',7:'h',8:'i',
9:'j',10:'k',11:'l',12:'m',13:'n',14:'o',15:'p',16:'q',17:'r',
18:'s',19:'t',20:'u',21:'v',22:'w',23:'x',24:'y',25:'z'}
```

```

k = 25
p=26

dic1 = {value: key for key, value in dic1.items()}
print(dic1)

string1 = 'HIALICE'
str1 = string1.lower()

nString = []
for i in range(len(str1)):
    nString.append(dic1[str1[i]])

print(nString)

for i in range(len(nString)):
    nString[i] = (nString[i]+k)%p

print(nString)

```

Listing 6: encrypting message

□

Exercise 6.7. Alice publishes the following public RSA key:

$$(n, e) = (1037266789560218962652439644600426307454279610255093794201383\,1, 2993534953779)$$

(a) Use Alice's public key to help Bob encrypt the following secret message to send to Alice:

$$k \equiv 91561593335933193354\,9$$

Hint: Copy and paste these numbers into Sage from the pdf or tex file.

(b) Later, Bob uses Alice's public key again to send another secret key. Help Eve break the cryptosystem and find the message he sent if his encrypted message was

$$39539521678984562782693181461023356030497818132397821402913\,29$$

Proof. (a) To encrypt the message k using (n, e), we must calculate $k^e \mod n$. Thus, our encrypted message is

$$\begin{aligned} m &\equiv (915615933359331933549)^{2993534953779} \\ &\equiv 2184301352343259510296055070545208232377058524462936828685410 \mod n \end{aligned}$$

(b) To decrypt this message we first must calculate e^{-1},

$$\begin{aligned} e^{-1} &\equiv e^{\varphi(\varphi(n))-1} \\ &\equiv 481372816268819517229933261704943697561637507924946484906581\,9 \mod \varphi(n) \end{aligned}$$

Now we must take the encrypted message and raise it to the power of e^{-1} and reduce modulo n which gives us the decrypted message of 9934537.

```

n = 10372667895602189626524396446004263074542796102550937942013831
e = 2993534953779
k = 915615933359331933549

m = pow(k, e, n)
print('Encrypted message: ',m)

phi_n = 10372667895602189626524396445992104708175688762026317476978000

```

```
        phi_phi_n = 41468404875219674390255179202373007840477222647214482419712 00

        inverse_e = pow(e,phi_phi_n-1,phi_n)

        print(inverse_e)

        decrypt_m = pow(m,inverse_e,n)

        m1 = 3953952167898456278269318146102335603049781813239782140291329

        k1 = pow(m1,inverse_e,n)

        print('k1: ',k1)

        print(pow(k1,e,n))


```

Listing 7: code for parts a and b(the Euler Phi values were calculated in Sage

□