Homework 3

CS 70, Summer 2024

Due by Friday, July 12$^{\text{th}}$ at 11:59 PM

1 Properties of the Greatest Common Divisor

(a) Since $a \mid c$ and $b \mid c$, there exist $k, j \in \mathbb{Z}$ such that

$$c = ak = bj.$$

By Bezout's identity, there exist $x, y \in \mathbb{Z}$ such that

$$\begin{aligned} ax + by &= \gcd(a, b) \\ ax + by &= 1 \\ cax + cby &= c \\ bjax + akby &= c \\ ab(jx + ky) &= c. \end{aligned}$$

Then $jx + ky \in \mathbb{Z}$ since $j, k, x, y \in \mathbb{Z}$. By definition, $ab \mid c$.

(b) Since $a \mid bc$, there exists $k \in \mathbb{Z}$ such that $bc = ak$. Again by Bezout's identity, there exist $x, y \in \mathbb{Z}$ such that

$$\begin{aligned} ax + by &= \gcd(a, b) \\ ax + by &= 1 \\ cax + cby &= c \\ acx + bcy &= c. \end{aligned}$$

Then $a \mid acx$ since $acx = a(cx)$ and $a \mid bc$ by assumption. Therefore, by **Lemma 1** of Note 7, $a \mid (acx + bcy)$, so $a \mid c$.

(c) By induction on n.

Base case. $n = 1$. If $\gcd(a_1, b) = 1$, then $\gcd(a_1, b) = 1$, as desired.

Induction case.

Induction hypothesis. For some $n \in \mathbb{N}^+$, suppose that for any integers $a_1, \ldots, a_n, b \in \mathbb{Z}$, if $\gcd(a_1, b) = \ldots = \gcd(a_n, b) = 1$, then $\gcd(a_1 \cdot \ldots \cdot a_n, b) = 1$.

Induction step. Consider any integers $a_1, \ldots, a_{n+1}, b \in \mathbb{Z}$ such that $\gcd(a_1, b) = \ldots = \gcd(a_n, b) = \gcd(a_{n+1}, b) = 1$.

Let $a = a_1 \cdot \ldots \cdot a_n$. By the induction hypothesis, $\gcd(a, b) = 1$. By Bezout's identity, there exist integers $x, y, u, v \in \mathbb{Z}$ such that

$$\begin{aligned} ax + by &= \gcd(a, b) = 1 \\ a_{n+1}u + bv &= \gcd(a_{n+1}, b) = 1. \end{aligned}$$

If we scale the second equation by a, we get that

$$aa_{n+1}u + abv = a.$$

Plugging this into the first equation gets us that

$$\begin{aligned} ax + by &= 1 \\ (aa_{n+1}u + abv)x + by &= 1 \\ aa_{n+1}(ux) + b(avx + y) &= 1. \end{aligned}$$

By **Lemma 1** from Note 7, for any divisor such that $d \mid (aa_{n+1}$ and $d \mid b$, we have that $d \mid (aa_{n+1}(ux) + b(avx + y)$. That is, $d \mid 1$. The only divisor of 1 is 1, so any divisor of both aa_{n+1} and b must be 1. That is,

$$\gcd(aa_{n+1}, b) = \gcd(a_1 \cdot \ldots \cdot a_n \cdot a_{n+1}, b) = 1.$$

By the principle of mathematical induction, we have shown that for any integers $a_1, \ldots, a_n, b \in \mathbb{Z}$, if $\gcd(a_1, b) = \ldots = \gcd(a_n, b) = 1$, then $\gcd(a_1 \cdot \ldots \cdot a_n, b) = 1$.

2 Existing Uniquely in the Chinese Remainder Theorem

(a) Let $M = m_1 \cdot \ldots \cdot m_n$ be the product of all the moduli and for each $i \in \{1, \ldots, n\}$, let $M_i = M/m_i$ be the product of all the moduli except for m_i.

Because $\gcd(m_i, m_j) = 1$ for all $i \neq j$ we have by Question 1**(c)** that $\gcd(M_i, m_i) = 1$. Therefore M_i has an inverse modulo m_i, so we can define

$$s_i = (M_i^{-1} \bmod m_i) \cdot M_i.$$

We construct our solution as

$$x = \sum_{i=1}^{n} a_i s_i.$$

Let us confirm that this yields a solution. For any $i \in \{1, \ldots, n\}$,

$$\begin{aligned}
x &\equiv \sum_{i=1}^{n} a_i s_i && \pmod{m_i} \\
&\equiv a_i s_i + \sum_{j \neq i}^{n} a_j s_i && \pmod{m_i} \\
&\equiv a_i \cdot (M_i^{-1} \bmod m_i) \cdot M_i + \sum_{j \neq i} a_j \cdot (M_j^{-1} \bmod m_j) \cdot M_j && \pmod{m_i} \\
&\equiv a_i \cdot M_i^{-1} \cdot M_i + \sum_{j \neq i} a_j \cdot (M_j^{-1} \bmod m_j) \cdot M_j && \pmod{m_i} \\
&\equiv a_i \cdot 1 + \sum_{j \neq i} a_j \cdot 0 && \pmod{m_i} \\
&\equiv a_i.
\end{aligned}$$

So x solves the system of congruences.

(b) By induction on n, the number of congruences.

Base case. $n = 1$. Then we only have the linear congruence $x \equiv a_1 \pmod{m_1}$, which has the solution $x = a_1 \bmod m_1$. For any other solution y, if $y \equiv a_1 \pmod{m_1}$, then $x \equiv y \pmod{m_1}$.

Induction case.

Induction hypothesis. For some $n \in \mathbb{N}^+$, suppose that any system of n linear congruences has a solution.

Induction step. Consider any system with $n + 1$ linear congruences. Consider any two solutions x and y. By the induction hypothesis, they are congruent modulo $m_1 \cdot \ldots \cdot m_n = m'$.

Therefore we have the system of equations

$$\begin{aligned}
x &\equiv y \pmod{m'} \\
x &\equiv y \pmod{m_{n+1}}.
\end{aligned}$$

Therefore $m' \mid (x - y)$ and $m_{n+1} \mid (x - y)$. By Question 1**(c)**, $\gcd(m', m_{n+1}) = 1$ and so by Question 1**(a)**, we have that $m' m_{n+1} \mid (x - y)$. So

$$x \equiv y \pmod{m' m_{n+1}}.$$

3 The Totient Function

(a) First, we will show that $r \bmod m \in S_m$.

By the Division Algorithm, we know that $r \bmod m \leq m$.

Since $r \in S_{mn}$, we have that $\gcd(r, mn) = 1$ by definition of S_{mn}.

We will prove $\gcd(r, m) = 1$ by contradiction as follows: Suppose $\gcd(r, m) = a$ for some $a > 1$. Then we know that $a \mid r$ and $a \mid m$, but this implies that $a \mid mn$ as well, which contradicts the fact that $\gcd(r, mn) = 1$.

Furthermore, we know that $\gcd(r, m) = \gcd(m, r \bmod m)$ (proven in Discussion 3A). Therefore, $\gcd(r \bmod m, m) = 1$.

Since $r \bmod m \leq m$ and $\gcd(r \bmod m, m) = 1$, $r \in S_m$ by definition of S_m.

We can apply an identical argument to conclude that $r \mod n \in S_n$.

Since r mod $m \in S_m$ and r mod $n \in S_n$, then $f(r) \in S_m \times S_n$.

(b) Suppose there exist two numbers $a, b \in S_{mn}$ where $f(a) = f(b) = (c, d)$.

This means that both a and b satisfy the following system of modular congruences:

$$x \equiv c \pmod{m}$$
$$x \equiv d \pmod{n}$$

However, the Chinese remainder theorem states that such a system of modular equivalences will have a unique solution modulo mn, so the fact that both a and b are between 0 and mn implies that $a = b$.

(c) For arbitrary element $(c, d) \in S_m \times S_n$, we can construct the following system of congruences:

$$r \equiv c \pmod{m}$$
$$r \equiv d \pmod{n}$$

By the Chinese Remainder Theorem, there exists some r that satisfies both congruences.

Furthermore, $\gcd(r, m) = \gcd(m, r \bmod m) = \gcd(r, c) = 1$, and one can apply an identical argument to show that $\gcd(r, n) = 1$.

Since $\gcd(r, m) = 1$ and $\gcd(r, n) = 1$, it must hold that $\gcd(r, mn) = 1$ and so $r \in S_{mn}$. Thus for any $(c, d) \in S_m \times S_n$, there exists some $r \in S_{mn}$ such that $f(r) = (c, d)$, and so f is a surjection.

(d) Since f is well-defined, is an injection, and is a surjection, it is a bijection from S_{mn} to $S_m \times S_n$. Therefore, $|S_{mn}| = |S_m \times S_n|$, and since both S_m and S_n are finite, $|S_m \times S_n| = |S_m||S_n|$. Therefore,

$$\varphi(mn) = |S_{mn}| = |S_m||S_n| = \varphi(m)\varphi(n).$$

4 Generalizing the Chinese Remainder Theorem

(a) If there is a solution to the system, then there exist integers x, k, ℓ such that $x = a + km = b + \ell n$. In other words, $a - b = km - \ell n$. But since $d \mid m$ and $d \mid n$, $d \mid km - \ell n$, proving the result.

(b) If $d \mid (a - b)$, then we can construct a solution by adapting the usual Chinese Remainder Theorem. By Bezout's lemma, we can write $d = fm + gn$. Then we claim $x = \frac{bfm+agn}{d}$ solves both equivalences. To see this, note that by rearrangement $\frac{fm}{d} = 1 - \frac{gn}{d}$.

$$x \equiv b\frac{fm}{d} + a\frac{gn}{d} \pmod{m}$$
$$x \equiv b\frac{fm}{d} + a - a\frac{fm}{d} \pmod{m}$$
$$x \equiv a - (a - b)\frac{fm}{d} \pmod{m}$$

Since $d \mid (a - b)$, we can write $kd = (a - b)$ for integer k. Thus, $x \equiv a - kfm \equiv a \pmod{m}$. Symmetrically one can show that $x \equiv b \pmod{n}$.

(c) Since c is a multiple of a and b, we have $c \geq \ell$. By the division algorithm, there exist integers q, r such that $c = q\ell + r$ where $0 \leq r < \ell$. Now, $r = c - q\ell$ and since c, ℓ are multiples of a and b we have $a \mid r$ and $b \mid r$. If $r \neq 0$, then r would be a smaller common multiple, which is a contradiction. Therefore, and $r = 0$ and $c = q\ell$, so $\ell \mid c$.

(d) Consider two solutions x, y to the system. Since $x \equiv y \pmod{m}$ and $x \equiv y \pmod{n}$, $m \mid (x - y)$ and $n \mid (x - y)$. By the previous part, we have that $\text{lcm}(m, n) \mid (x - y)$. Therefore, $x - y \equiv 0 \pmod{\text{lcm}(m, n)}$ or that they are equal up to this modulo. Therefore, solutions are unique up to this modulo.

(e) We can calculate the solution for two congruences as follows: $d = \gcd(m_1, m_2)$. Then, a unique solution modulo $\text{lcm}(m_1, m_2)$ exists as long as $m_1 \equiv m_2 \pmod{d}$. To construct the unique solution, we write the linear combination using Bezout's. To construct it, one can just compute, for each i from 1 to n

$$f \equiv \left(\frac{m_2}{d}\right)^{-1} \pmod{m_1/d}$$
$$g \equiv \left(\frac{m_1}{d}\right)^{-1} \pmod{m_2/d}$$

Then, we can construct the solution as in (b). Now, we can replace these two congruences with a new congruence modulo $\text{lcm}(m_1, m_2)$ and repeat until there is only one congruence left.

(f) $\gcd(2,4) = 2$ and $\text{lcm}(2,4) = 4$. Here we can easily write $2 = (1)(2) + (0)(4)$, yielding $f = 1$ and $g = 0$. Thus, our intermediate $x \equiv \frac{2 \cdot 1 \cdot 2 + 0 \cdot 0 \cdot 4}{2} \equiv 2 \pmod 4$.

Next, we will combine the bottom two recurrences. Here, the usual CRT suffices, finding $1 = (7)(13) + (-5)(18)$ with Euclid's algorithm. Since $13 \cdot 18 = 234$ this yields $x \equiv (4)(7)(13) + (2)(-5)(18) \equiv 364 - 180 \equiv 184 \pmod{234}$. Finally, $\gcd(4, 234) = 2$ and $\text{lcm}(4, 234) = 2 \cdot 234 = 468$, and again we can write 2 and 117 with Bezout's as $1 = (-58)(2) + (1)(117)$ so $2 = (-58)(4) + (1)(234)$. Therefore

$$x \equiv \frac{(184)(-58)(4) + (2)(1)(234)}{2} \equiv 418 \pmod{468}$$

5 RSA Prime Counts

(a) We pick $d \equiv e^{-1} \pmod{p-1}$. Then $D(y) = y^d \mod p$. Now, $D(E(x)) = x^{ed} \mod p$. Since $ed \equiv 1 \pmod{p-1}$, then there exists integer such that $ed = 1 + k(p-1)$. Then

$$D(E(x)) \equiv x \cdot \left(x^{p-1}\right)^k \equiv x \cdot 1^k \equiv 1 \pmod p$$

where the second-to-last step used FLT.

(b) The public key will just be the prime $N = p$, so we can calculate $p - 1$ easily and compute d to decrypt messages.

(c) We pick $d \equiv e^{-1} \pmod{(p-1)(q-1)(r-1)}$. Then $D(y) = y^d \mod N$. Now, we will show that encryption and decryption recovers the original message, e.g. $D(E(x)) = x$. We find $D(E(x)) = x^{ed} \mod N$. Since $ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$, then there exists integer such that $ed = 1 + k(p-1)(q-1)(r-1)$. Then

$$D(E(x)) \equiv x \cdot \left(x^{p-1}\right)^{k(q-1)(r-1)} \equiv x \cdot 1^k \equiv x \pmod p$$

Similarly, $D(E(x)) \equiv x \pmod q$ and $D(E(x)) \equiv x \pmod r$. By the Chinese Remainder Theorem, there is a unique solution for x modulo pqr (distinct primes are coprime). One can see that if $D(E(x)) \equiv x \pmod{pqr}$ then clearly $D(E(x)) \equiv x \pmod p$ and for q, r as well, so this is the solution we get. Thus, the encryption scheme works.

(d) Similar to regular RSA, one would need to somehow factor $N = pqr$ into p, q, r to get $(p-1), (q-1), (r-1)$ in order to then find the modulo to invert e. The previous attack required no factoring, just a subtraction, which is easy.

6 Euler's Theorem

(a) All the integers between 1 and $p-1$ inclusive are coprime to a prime p, so $\varphi(p) = p-1$. The theorem thus asks whether $a^{p-1} \equiv 1$ for a coprime to p (i.e. $a \not\equiv 0 \pmod p$). This is exactly Fermat's Last Theorem, so that is enough to prove this case.

(b) By Question 1**(c)**, since $\gcd(a, m) = 1$ and $\gcd(x, m) = 1$, we have that $\gcd(ax, m) = 1$. By the Euclidean algorithm, $\gcd(ax \mod m, m) = 1$, so $ax \mod m \in S_m$.

(c) We must show that f is an injection and that f is a bijection.

f is an injection. For any $x_1, x_2 \in S_m$, suppose that $f(x_1) = f(x_2)$. Then $ax_1 \mod m = ax_2 \mod m$, so $ax_1 \equiv ax_2 \pmod m$. Since $\gcd(a, m) = 1$, a^{-1} exists modulo m and hence $x_1 \equiv x_2 \pmod m$. That is, $m \mid (x_1 - x_2)$. In particular, $x_1 - x_k = mk$ for some $k \in \mathbb{Z}$. However, since $0 \le x_1, x_2 < m$, we have that $-m < x_1 - x_2 < m$. So we cannot have that $k \ge 1$ nor can we have that $k \le -1$, so it must be that $k = 0$ and hence $x_1 = x_2$.

f is a surjection. For any $y \in S_m$, consider the $x = (a^{-1} \mod m)y$. Then $f(x) = a(a^{-1} \mod m)y \mod m = y$. Moreover, since a^{-1} has an inverse modulo m, we know that $\gcd(a^{-1} \mod m, m) = 1$. Then, since $\gcd(y, m) = 1$, we have that $\gcd((a^{-1} \mod m)y, m) = 1$, and so $x \in S_m$.

(d) Since f is a bijection, the set $\{ax \pmod m : x \in S_m\} = S_m$. Now, consider multiplying all of these elements. On the left side, we get $\prod_{x \in S_m} ax = a^{|S_m|} \prod_{x \in S_m} x = a^{\varphi(m)} \prod_{x \in S_m}$. On the right side, we get $\prod_{x \in S_m} x$. Setting these equal, we get

$$a^{\varphi(m)} \left(\prod_{x \in S_m} x \right) \equiv \prod_{x \in S_m} x \pmod m$$
$$a^{\varphi(m)} \equiv 1 \pmod m$$

where in the last step, we were able to take inverses of each element in the product since they were in S_m and thus coprime to m.