Due Wednesday Sept 30 at 10PM

1. **Bijections**

   Let n be an odd number. Let $f(x)$ be a function from $\{0,1,\ldots,n-1\}$ to $\{0,1,\ldots,n-1\}$. In each of these cases say whether or not $f(x)$ is a bijection. Justify your answer (either prove $f(x)$ is a bijection or give a counterexample).

   (a) $f(x) = 2x \pmod{n}$.

   Answer: Bijection, because there exists the inverse function $g(y) = 2^{-1}y \pmod{n}$ (See Lemma 7.1 from Lecture note 7). Since n is odd, $gcd(2,n) = 1$, so the multiplicative inverse of 2 exists (See Theorem 6.2 from Lecture note 6).

   (b) $f(x) = 5x \pmod{n}$.

   Answer: Not a bijection. For example, $n = 5, f(0) = f(1) = 0$.

   (c) n is prime and

   $$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ x^{-1} \pmod{n} & \text{if } x \neq 0 \end{cases}$$

   Answer: Bijection, because the multiplicative inverse is unique (Theorem 6.2).

   (d) n is prime and $f(x) = x^2 \pmod{n}$.

   Answer: Not a bijection. For example, if n = 3, f (1) = f (2) = 1.

2. **Fermat's Little Theorem**

   Fermat's Little Theorem in Lecture Note 7 [Theorem 7.1] states that for any prime p and any $a \in \{1,2,..p-1\}$, we have $a^{p-1} \equiv 1 (\bmod p)$. Without using induction, prove that $\forall n \in \mathbb{N}$, $n^7 - n$ is divisible by 42.

   Answer: We begin by breaking down 42 into prime factors: $42 = 7 \times 3 \times 2$. Since 7,3, and 2 are prime, we can apply Fermat's Little Theorem, which says that $a^p \equiv a \pmod{p}$, to get the congruences

   $$n^7 \equiv n(\bmod 7), \quad (1)$$
   $$n^3 \equiv n(\bmod 3), \text{ and} \quad (2)$$
   $$n^2 \equiv n(\bmod 2). \quad (3)$$

   Now, let's take (2) and multiply it by $n^3 \cdot n$. This gives us

   $$n^7 \equiv n^3 \cdot n^3 \cdot n \equiv n \cdot n \cdot n \equiv n^3 \pmod{3},$$

   and since by (2), $n^3 \equiv n \pmod{3}$, this gives

   $$n^7 \equiv n \pmod{3}.$$

Similarly, we take (3) and multiply by $n^2 \cdot n^2 \cdot n$ to get

$$n^7 \equiv n^2 \cdot n^2 \cdot n^2 \cdot n \equiv n^4 \pmod 2.$$

Notice that $n^4 \equiv n^2 \cdot n^2 \equiv n \cdot n \equiv n^2 \pmod 2$, and by (3) $n^2 \equiv n \pmod 2$, so we have

$$n^7 \equiv n \pmod 2.$$

Thus,

$$n^7 \equiv n \pmod 7, \tag{4}$$
$$n^7 \equiv n \pmod 3, \text{ and} \tag{5}$$
$$n^7 \equiv n \pmod 2. \tag{6}$$

Lemma 1. If $x \equiv y \pmod{a_i}$, for $1 \le i \le k$, and $a_1, a_2, ..., a_k$ are co-prime, then $x \equiv y \pmod{a_1 a_2 ... a_k}$.

Proof. When $x \equiv y \pmod{a_i}$, for $1 \le i \le k$, we know that $x = c \times lcm(a_1, a_2, ..., a_k) + y$ for some integer c. (lcm is *least common multiple*.)
Since $a_1, a_2, ..., a_k$ are co-prime, $lcm(a_1, a_2, ..., a_k) = a_1 a_2 ... a_k$, so $x = c \times a_1 a_2 ... a_k + y$.
Thus, $x \equiv y \pmod{a_1 a_2 ... a_k}$. □

Alternative proof. For every i, since $x \equiv y \pmod{a_i}$, $x = y + c_i a_i$ where c_i is integer, so $x - y = c_i a_i$.
Thus, $(x-y)^k = c_1 c_2 ... c_k \times a_1 a_2 ... a_k$.
Since $a_1, a_2, ..., a_k$ are co-prime, $x - y = c \times a_1 a_2 ... a_k$ for some integer c.
Hence, $x \equiv y \pmod{a_1 a_2 ... a_k}$. □

Apply Lemma 1 on (4), (5), and (6), we have that $n^7 \equiv n \pmod{7 \times 3 \times 2}$, so $n^7 \equiv n \pmod{42}$. Subtracting n from both sides of the congruence gives $n^7 - n \equiv 0 \pmod{42}$, which means $n^7 - n$ is divisible by 42.

3. **Tweaking RSA**

   (a) You are trying to send a message to your friend, and as usual, Eve is trying to decipher what the message is. However, you get lazy, so you use $N = p$, and p is prime. Similar to the original method, for any message $x \in \{0, 1, \dots, N-1\}$, $E(x) \equiv x^e \pmod N$, and $D(y) \equiv y^d \pmod N$. Show how you choose e and d in the encryption and decryption function, respectively. Prove that the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

   Answer: Choose e such that it is coprime with $p-1$, and choose $d \equiv e^{-1} \pmod{p-1}$.
   We want to show x is recovered by $E(x)$ and $D(y)$, such that $D(E(x)) = x$.
   In other words, $x^{ed} \equiv x \pmod p$ $\forall x \in \{0, 1, \dots, N-1\}$.
   Proof: By construction of d, we know that $ed \equiv 1 \pmod{p-1}$. This means we can write $ed = k(p-1)+1$, for some integer k, and $x^{ed} = x^{k(p-1)+1}$.

   - x is a multiple of p: Then this means $x = 0$, and indeed, $x^{ed} \equiv 0 \pmod p$.
   - x is not a multiple of p: Then $x^{ed} \equiv x^{k(p-1)+1} \equiv x^{k(p-1)} x \equiv 1^k x \equiv x \pmod p$, by using FLT.

   And for both cases, we have shown that x is recovered by $E(D(y))$.

   (b) Can Eve now compute d in the decryption function? If so, by what algorithm?

   Answer: Since Eve knows $N = p$, and $d \equiv e^{-1} \pmod{p-1}$, now she can compute d using EGCD.

(c) Now you wonder if you can modify the RSA encryption method to work with three primes ($N = pqr$ where p, q, r are all prime). Explain how you can do so.

Answer: Let e be co-prime with $(p-1)(q-1)(r-1)$. Give the public key: (N, e) and calculate $d = e^{-1} \bmod (p-1)(q-1)(r-1)$. People who wish to send me a secret, x, send $y = x^e \bmod N$. We decrypt an incoming message, y, by calculating $y^d \bmod N$.

Does this work? We prove that $x^{ed} - x \equiv 0 \bmod N$, and thus $x^{ed} = x \bmod N$.

To prove that $x^{ed} - x \equiv 0 \bmod N$, we factor out the x to get
$x \cdot (x^{ed-1} - 1) = x \cdot (x^{k(p-1)(q-1)(r-1)+1-1} - 1)$ because $ed \equiv 1 \bmod (p-1)(q-1)(r-1)$.

We now show that $x \cdot (x^{k(p-1)(q-1)(r-1)} - 1)$ is divisible by p, q, and r. Thus, it is divisible by N, and $x^{ed} - x \equiv 0 \bmod N$.

To prove that it is divisible by p:

- if x is divisible by p, then the entire thing is divisible by p.
- if x is not divisible by p, then that means we can use FLT on the inside to show that $(x^{p-1})^{k(q-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \bmod p$. Thus it is divisible by p.

To prove that it is divisible by q:

- if x is divisible by q, then the entire thing is divisible by q.
- if x is not divisible by q, then that means we can use FLT on the inside to show that $(x^{q-1})^{k(p-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \bmod q$. Thus it is divisible by q.

To prove that it is divisible by r:

- if x is divisible by r, then the entire thing is divisible by r.
- if x is not divisible by r, then that means we can use FLT on the inside to show that $(x^{r-1})^{k(p-1)(q-1)} - 1 \equiv 1 - 1 \equiv 0 \bmod r$. Thus it is divisible by r.

4. **Digital Signatures**

The RSA crypto system can be used to implement a digital signature scheme. It allows Bob to sign a document m and give Alice $S(m)$ which satisfies the following properties:

(i) If Bob gives the signed document $S(m)$ to Alice, she can verify that Bob signed the document.

(ii) Alice can show $S(m)$ to Carol and convince her that this a copy of document m signed by Bob.

(iii) No one other than Bob can forge his signature on a document.

In this problem:

(a) Show that using Bob's RSA decryption function on m to create $S(m)$ satisfies the first two properties.

Answer: Let E and D denote Bob's encryption and decryption function respectively. Since D and E are inverses of each other, $E(D(m)) = D(E(m)) = m$. Therefore, if Alice receives the signed document $S(m)$, she can verify that Bob signed the document by simply applying the encryption function E to it and checking that m comes back out. Note that this verification can be carried out by anyone who has Bob's public key and the original document m. Therefore the first two properties are immediately satisfied.

(b) Using Bob's RSA decryption function also comes close to satisfying the third property, but not quite. For example, Alice can pick an arbitrary input x, encrypt it using Bob's key and call the result $E(x) = m$. Now if Bob is using his RSA decryption function as the signature, then Alice knows that $S(m) = x$, so Alice can pretend to be Bob sending the document m.

Give a small modification to make the scheme secure against this type of attack. Give an informal justification that your scheme is secure.

Answer: For instance, one can propose that Bob first concatenates the message m with a string of 0's of the same length as m, and then applies his RSA decryption function to the resulting string to produce his signed document. Whoever has Bob's public key and the original document m can verify the authenticity of the signature by checking that Bob's RSA encryption function returns m concatenated with the right number of 0's. Since Alice does not have any control over the format of $E(x)$ in the proposed attack, the scheme is secure against this attack.

5. **Secret Sharing**

Suppose we wish to share a secret among five people, and we decide to work modulo 7. We construct a degree-two polynomial $q(x) = ax^2 + bx + s$ by picking the coefficients a and b at random (mod 7); the constant term is the secret s (also a number mod 7). We give shares $q(1), \ldots, q(5)$ to each of the five people (all operations being done mod 7). Now suppose that three of the people get together and share the information that $q(1) = 5$, $q(2) = 2$, and $q(4) = 2$. Use Lagrange interpolation to find the polynomial q and the secret s. Show all your work.

Answer: For convenience, we will first list the inverse pairs modulo 7: $(1,1),(2,4),(3,5),(6,6)$. Now, to find a polynomial q such that $q(1) = 5$, $q(2) = 2$, and $q(4) = 2$, we must compute

$$q(x) = 5\Delta_1(x) + 2\Delta_2(x) + 2\Delta_4(x),$$

where each Δ_i is computed as follows:

$$\begin{aligned}
\Delta_1 &= \frac{(x-2)(x-4)}{(1-2)(1-4)} = \frac{x^2-6x+8}{(-1)(-3)} = 5(x^2+x+1) = 5x^2+5x+5 \\
\Delta_2 &= \frac{(x-1)(x-4)}{(2-1)(2-4)} = \frac{x^2-5x+4}{(1)(-2)} = 3(x^2+2x+4) = 3x^2+6x+5 \\
\Delta_4 &= \frac{(x-1)(x-2)}{(4-1)(4-2)} = \frac{x^2-3x+2}{(3)(2)} = 6(x^2+4x+2) = 6x^2+3x+5
\end{aligned}$$

Substituting, we now have

$$\begin{aligned}
q(x) &= 5(5x^2+5x+5) + 2(3x^2+6x+5) + 2(6x^2+3x+5) \\
&= (4x^2+4x+4) + (6x^2+5x+3) + (5x^2+6x+3) \\
&= x^2+x+3
\end{aligned}$$

6. **Properties of $GF(p)$**

(a) Show that, if $p(x)$ and $q(x)$ are polynomials over the reals (or complex, or rationals) and $p(x) \cdot q(x) = 0$ for all x, then either $p(x) = 0$ for all x or $q(x) = 0$ for all x or both.

Answer: We will show the contrapositive. Suppose that $p(x)$ and $q(x)$ are both non-zero polynomials of degree d_p and d_q respectively. Then $p(x) = 0$ for at most d_p values of x and $q(x) = 0$ for at most d_q values of x. Since there are an infinite number of values for x (because we are using complex, real, or rational numbers) we can always find an x, call it $x_{notzero!}$, for which $p(x_{notzero!}) \neq 0$ and $q(x_{notzero!}) \neq 0$. This gives us $p(x_{notzero!}) \cdot q(x_{notzero}) \neq 0$, so pq is non-zero.

(b) Show that the claim in part (a) is false for finite fields $GF(p)$.

Answer: In $GF(p)$, $x^{p-1}-1$ and x are both non zero polynomials, but when p is prime, their product $(x^p - x)$ is zero for all x by Fermat's little Theorem.

7. **GCD of Polynomials**

Let $A(x)$ and $B(x)$ be polynomials (with coefficients in $\mathbb{R}$ or $GF(m)$). We say that $\gcd(A(x),B(x)) = D(x)$ if $D(x)$ divides $A(x)$ and $B(x)$, and if every polynomial $C(x)$ that divides both $A(x)$ and $B(x)$ also divides $D(x)$. For example, $\gcd((x-1)(x+1),(x-1)(x+2)) = x-1$. Incidentally, $\gcd(A(x),B(x))$ is the highest degree polynomial that divides both $A(x)$ and $B(x)$.

(a) Write a recursive program to compute $gcd(A(x),B(x))$. You may assume you already have a subroutine for dividing two polynomials.

Answer: Specifically, we wish to find a gcd of two polynomials $A(x)$ and $B(x)$, assuming that that $\deg A(x) \geq \deg B(x) > 0$. Here, $\deg A(x)$ denotes the degree of $A(x)$.

We can find two polynomials $Q_0(x)$ and $R_0(x)$ by polynomial long division (see lecture note 8) which satisfy

$$A(x) = B(x)Q_0(x) + R_0(x), \qquad 0 \leq \deg R_0(x) < \deg B(x)$$

Notice that a polynomial $C(x)$ divides $A(x)$ and $B(x)$ iff it divides $B(x)$ and $R_0(x)$.

[Proof: $C(x)$ divides $A(x), B(x)$, there $\exists S(x)$ and $S'(x)$ s.t. $A(x) = C(x)S(x)$ and $B(x) = C(x)S'(x)$, so $R_0(x) = A(x) - B(x)Q_0(x) = C(x)(S(x) - S'(x)Q_0(x))$, therefore $C(x)$ divides $R_0(x)$ or $R_0(x) = 0$.]

We deduce that

$$gcd(A(x),B(x)) = gcd(B(x),R(x))$$

and set $A_1(x) = B_1(x), B_1(x) = R_0(x)$; we then repeat to get new polynomials $Q_1(x), R_1(x), A_2(x), B_2(x)$ and so on. The degrees of the polynomials keep getting smaller and will eventually reach a point at which $B_N(x) = 0$; and we will have found our gcd:

$$gcd(A(x),B(x)) = gcd(A_1(x),B_1(x)) = \cdots = gcd(A_N(x),0) = A_N(x)$$

Here, we have the function that can perform the polynomial long division on $A(x)$ and $B(x)$ and return both the quotient $Q(x)$ and the remainder $R(x)$, i.e. $[Q(x), R(x)]$ = div$(A(x),B(x))$. The algorithm can be extended from the original integer-based GCD as follows:

```
function gcd(A(x), B(x)):
  if B(x) = 0:
    return A(x)
  else if deg A(x) < deg B(x):
    return gcd(B(x), A(x))
  else:
    (Q(x), R(x)) = div(A(x), B(x))
    return gcd(B(x), R(x))
```

(b) Let $P(x) = x^4 - 1$ and $Q(x) = x^3 + x^2$ in standard form. Prove there are no polynomials $A(x)$ and $B(x)$ such that $A(x)P(x) + B(x)Q(x) = 1$ for all x.

Answer: We can compute a gcd of $P(x)$ and $Q(x)$ using the algorithm in part (a), and show that it is not 1.

$$\begin{aligned}
gcd(x^4-1, \quad x^3+x^2) \quad & // \quad x^4-1=(x^3+x^2)(x-1)+(x^2-1) \\
gcd(x^3+x^2, \quad x^2-1) \quad & // \quad x^3+x^2=(x^2-1)(x+1)+(x+1) \\
gcd(x^2-1, \quad x+1) \quad & // \quad x^2-1=(x+1)(x-1)+0 \\
gcd(x+1, \quad 0) \quad & // \quad D(x)=x+1
\end{aligned}$$

We can also derive that $gcd(P(x),Q(x))$ has the smallest degree among all the polynomials that can be expressed as a linear combination of $P(x)$ and $Q(x)$ (see proof below). And since 1 is of degree 0, which is smaller than 1, the degree of $gcd(P(x),Q(x)) = x+1$, there exists no such linear combination.

[Consider the following set:

$$I = \{S(x)P(x)+T(x)Q(x) : S(x),T(x) \text{in the same field as} P(x),Q(x)\}$$

Pick a polynomial $D(x) \in I$ of the smallest degree. We have

$$D(x) = S(x)P(x)+T(x)Q(x) \tag{7}$$

We want to show that

- $D(x)$ is a common divisor of $P(x)$ and $Q(x)$.
- Any common divisor of $P(x)$ and $Q(x)$ must divides $D(x)$.

If these two properties hold, $D(x) = gcd(P(x),Q(x))$.

From polynomial long division of $P(x)$ and $D(x)$, we also obtain

$$P(x) = D(x)E(x)+R(x) \tag{8}$$

where $E(x)$ is the quotient and the remainder $R(x)$ can either be 0 or has $\deg R(x) < \deg D(x)$.From (7) and (8), it follows that

$$\begin{aligned}
R(x) = P(x) - D(x)E(x) &= P(x) - [S(x)P(x)+T(x)Q(x)] \cdot E(x) && (9) \\
&= [1-S(x)E(x)] \cdot P(x) - [T(x)E(x)] \cdot Q(x) && (10)
\end{aligned}$$

So $R(x)$ is also a linear combination of $P(x)$ and $Q(x)$, but $D(x)$ is defined to have the smallest degree; therefore $R(x) = 0$, which means that $D(x)$ divides $P(x)$. A similar argument shows that $D(x)$ divides $Q(x)$.

We now want to show that any common divisor $C(x)$ of $P(x)$ and $Q(x)$ must divide $D(x)$.

Let $P(x) = C(x)P'(x)$ and $Q(x) = C(x)Q'(x)$. We have that $D(x) = S(x)C(x)P'(x)+T(x)C(x)Q'(x) = C(x)[S(x)P'(x)+T(x)Q'(x)]$, so C(x) divides D(x).

Therefore, $D(x)$ is the greatest common divisor of $P(x)$ and $Q(x)$, and is of the form $S(x)P(x)+T(x)Q(x)$.

Alternative proof.

Proof by contradiction. Assume that there is $A(x)$ and $B(x)$ such that $A(x)P(x)+B(x)Q(x) = 1$. We know that $gcd(P,Q) = x+1$, so:

$$A(x)P(x)+B(x)Q(x) = (x+1)[A(x)P'(x)+B(x)Q'(x)] = 1$$

Let $A(x)P'(x)+B(x)Q'(x) = Z(x)$. $(x+1)Z(x)$ is then a polynomial of degree at least 1. However, there is no polynomial $Z(x)$ such that $(x+1)Z(x) = 1$. Contradict! Therefore, there is no $A(x)$ and $B(x)$ such that $A(x)P(x)+B(x)Q(x) = 1$.]

(c) Find polynomials $A(x)$ and $B(x)$ such that $A(x)P(x)+B(x)Q(x)=x+1$ for all x.

Answer: Using extended gcd for polynomials, we can work our way backwards from the result of part (b) to find $A(x)$ and $B(x)$. We know that

$$x+1=(x^3+x^2)-(x+1)(x^2-1)$$

Plugging in the formula for x^2-1, we get

$$\begin{aligned} x+1 &= (x^3+x^2)-(x+1)[(x^4-1)-(x^3+x^2)(x-1)] \\ &= -(x+1)(x^4-1)+x^2(x^3+x^2) \end{aligned}$$

So therefore, $A(x)=-(x+1)$ and $B(x)=x^2$.