Ilana Sivan
205634272
Honors Course
Homework 4

Question 1

We will define:
$\mathbb{Z}_N \coloneqq \{0, 1, ..., N-1\}$
$\mathbb{Z}_N \coloneqq \{x \in \mathbb{Z}_N | \exists y \in \mathbb{Z}_N, xy \equiv 1 (\mathrm{mod} N)\}$

a. If p is prime, what is $|\mathbb{Z}^*_{\mathrm{p^n}}|$? In other words, for how many elements of the group $|\mathbb{Z}^*_{\mathrm{p^n}}|$ there is an inverse modulo p^n?

Similar to our proofs from last week, if p is indeed a prime, then we know that $\mathrm{p^n}$ has only one factor, p. The only numbers in $|\mathbb{Z}^*_{\mathrm{p^n}}|$ that have a common factor of p^n are: $\{p, 2p, ..., p^n - p\}$. We define $f(i) = \frac{i}{p}$, which is a bijective function, and we get the set $\{1, 2, ...p^{n-1} - 1\}$. We know from last week's solution that we exclude all the numbers which are multiples of p. In fact, since p is a prime, all elements in the range that are not a multiple of p have an inverse of $\mathrm{modp^n}$. If we count the numbers in the set we get $p^{n-1} - 1$ numbers, and if we subtract it from the total size of $\mathbb{Z}^*_{\mathrm{p^n}}$ we get $|\mathbb{Z}^*_{\mathrm{p^n}}| = p^n - 1 - (p^{n-1} - 1) = p^n - 1 - p^{n-1} + 1 = p^n - p^{n-1}$, so as last week, we get $\mathrm{p^n - p^{n-1}}$.

b. If p, q are prime, what is $|\mathbb{Z}^*_{\mathrm{pq}}|$?

If we observe the set, we can see that $\gcd(\mathrm{x}, \mathrm{pq}) = 1$ **iff** $\mathrm{x} \not\equiv 0 \mathrm{modp}$ **and** $\mathrm{x} \not\equiv 0 \mathrm{modq}$. We would like to find all the numbers for which this holds. For every $x \in \mathbb{Z}^*_{\mathrm{pq}}$ if x is a multiple of p or q, then $\gcd(\mathrm{x}, \mathrm{pq}) \neq 1$ so the range is $\{0, 1, ...pq - 1\}$ so there are pnumbers that are multiples of q, and q numbers which are multiples of p. Due to the inclusion of 0 twice we have the following solution:
$|\mathbb{Z}^*_{\mathrm{pq}}| = |\mathbb{Z}_{\mathrm{pq}}| - p - q + 1 = pq - p - q + 1$

Question 2

Give a polynomial-time algorithm for computing $\mathrm{a}^{\mathrm{b}^{\mathrm{c}}}\mathrm{mod p}$, given $\mathrm{a}, \mathrm{b}, \mathrm{c}$, and prime p.

An algorithm is defined as polynomial if its run time is $O(n^c)$ where c is some constant, for inputs of length n. Our algorithm will use multiplication (squaring) and computations.

We will construct our algorithm by using Fermat's theorem: $\mathrm{a}^{\mathrm{p}-1}\mathrm{mod}p = 1$, from there it follows that we can use the following equation: $\mathrm{a}^{\mathrm{b}^{\mathrm{c}}}\mathrm{mod}p = \mathrm{a}^{\mathrm{b}^{\mathrm{c}}\mathrm{mod(p=1)}}\mathrm{mod}p$. We further note, that if a is in fact divisible by p, then $\mathrm{a}^{\mathrm{b}^{\mathrm{c}}}\mathrm{mod}p = 0^{\mathrm{b}^{\mathrm{c}}\mathrm{mod(p=1)}}\mathrm{mod}p$.

Our algorithm is as follows:

1. Compute $\mathrm{bmod(p-1)}$
2. Compute $\mathrm{b^c mod(p-1)}$ with repeated squaring
3. Compute $\mathrm{amod(p)}$
4. Compute $\mathrm{a}^{\mathrm{b}^{\mathrm{c}}}\mathrm{mod}p$ with repeated squaring

Our first step is in $O(\log b \log p)$. Our second step, assuming that each multiplication of numbers between 0 and p is in $O(\log c)$, we then will take the result of this modulo p-1 for $O(\log^2 p)$ time, for a total of $O(\log c \log^2 p)$. Our third step is in $O(\log a \log p)$. And our final step is in $O(\log p \log p^2) = O(\log^3 p)$, but we note that $\mathrm{b^c mod(p-1)} < \mathrm{p}$. Therefore, our total running time is $O(\log b \log p + \log c \log^2 p + \log a \log p + \log^3 p)$. From this it follows that we are upperbounded by $O(n^3)$.

Another possible solution is to compute immediately $\mathrm{b^c mod(p-1)}$ for a runtime of $O(\log c \log^2 p + \log b \log p)$, then $\mathrm{a}^{\mathrm{b}^{\mathrm{c}}}\mathrm{mod}p$ with repeated squaring and the same conditions on $\mathrm{b^c mod(p-1)} < \mathrm{p}$, for a runtime of $O(\log p \log^2 p + \log a \log p)$, for a total runtime of $O(\log b \log p + \log c \log^2 p + \log a \log p + \log^3 p)$. As the runtime is the same and bounded by $O(n^3)$, these two solutions are basically the same, but I found it easier to take each step individually in calculating.

Question 3

Wilson's theorem says that a number N is prime if and only if :
$(\mathrm{N}-1)! \equiv -1(\mathrm{modN})$

a. If p is prime, then for every number $1 \leq \mathrm{x} < \mathrm{p}$ there is an inverse modulo. Which of these numbers are their own inverse?

For a number x, defined by $1 \leq \mathrm{x} < \mathrm{p}$ to be its own inverse modulo, then the following statement must hold: $\mathrm{x}^2 \equiv 1(\mathrm{modp})$, the equivalence of this congruence is equivalent to $\mathrm{x}^2 - 1 \equiv 0\mathrm{modp}$, so therefore, we need $\mathrm{x} \equiv \pm 1(\mathrm{modp})$ when p is some prime. We factor and we can see that $(\mathrm{x}+1)(\mathrm{x}-1) = 0\mathrm{modp}$, so we have either $\mathrm{x}+1$ or $\mathrm{x}-1$ are 0mod p. Therefore, 1 and $p-1$ are their own inverse modulos.

b. Pair up numbers and their inverses and show that for every prime p, there exists $(\mathrm{p}-1)! \equiv -1(\mathrm{modp})$

One can pair all numbers apart from 1 and $p-1$ (from part a) with a multiplicative inverse, so $(\mathrm{p}-1)! \equiv \mathrm{p}-1 \equiv -1\mathrm{modp}$.

We know that for a prime number p, every positive integer less than this number is considered to be coprime to p, and every integer in the set which we denote as $\mathbb{Z}_{\mathrm{p}}^*$ has an inverse in $\mathbb{Z}_{\mathrm{p}}$. Let b_p be the inverse of a_p, then we get $a_p b_p = 1_p$, so we can see that $ab_p = 1_p$, that is to say, that $ab = 1 \mathrm{mod} p$. As we know from part a, the solution to $\mathrm{x}^2 \equiv 1(\mathrm{modp})$ is $(\mathrm{x}+1)(\mathrm{x}-1) = 0\mathrm{modp}$, that is to say that $\mathrm{x} \equiv \pm 1$ and that these values $1, -1 = p-1$ are inverses of themselves. So for other values of x we know that the inverse of x is not equal to x. So for all other elements of $\mathbb{Z}_{\mathrm{p}}^*$, we can divide it into $\frac{p-3}{2}$ pairs of $(\mathrm{x}, \mathrm{x}^{-1})$, the product of which is 1. For $\mathrm{p} = 2$ the statement holds as $(2-1) = 1 \equiv 1!\mathrm{modp}$, which is true, and finally for every $\mathrm{p} > 2$:
$(\mathrm{p}-1)! = 1 * 2 * ... * (\mathrm{p}-1) \equiv 1 * 1 * ... * (\mathrm{p}-1) \equiv -1(\mathrm{modp})$
or as before, $(\mathrm{p}-1)! \equiv \mathrm{p}-1 \equiv -1\mathrm{modp}$.

c. Show that if N is not prime, then $(N-1)! \not\equiv -1 (\mathrm{mod} N)$. Hint: look at $\gcd(N, (N-1))$

If N is composite, then it may have at least one prime factor $\mathrm{p} < \mathrm{N}$ which is a divisor of $(\mathrm{N}-1)! = \mathrm{cN} + \mathrm{d}$. As p is a divisor of N and $\mathrm{N}-1$, it must also divide d. Therefore, $\mathrm{d} = -1$ is not a possible solution. In the case of $\mathrm{N} = 1$, we have $(1-1)! = 0! = 1 \equiv -1\mathrm{mod}1$, where our remainder is 0 (and not -1). So $\mathrm{N} = 1$ is not a solution. We can further consider $\gcd(\mathrm{N}, (\mathrm{N}-1)!)$, if our N is not prime, then it must be comprised of two numbers, $\mathrm{a}, \mathrm{b} < \mathrm{N}$. So, $\mathrm{N}-1!$ is a multiple of N, that is to say that $(\mathrm{N}-1)! = 0\mathrm{mod}\mathrm{N}$.

d. Unlike Fermat's theorem, Wilson's theorem has a a condition a necessary and sufficient condition for primality. If this is so, why will there be a problem basing a test on primality with this rule?

Wilson's theorem is computationally expensive. As it states that N is prime **iff** $(\mathrm{N}-1)! \equiv -1\mathrm{mod}\mathrm{N}$, it requires N modular multiplications. So while Wilson's theorem is fine to test primarity for small values, it is not practical to base primality testing on it for large values as the factorial grows too rapidly in the necessary conditions, in fact a three digit N will yield over a hundred digits in $(\mathrm{N}-1)!$

Question 4

In this question we will prove the Chinese Remainder theorem for the product of two different primes.

a. Make a table with three columns. In the first column write all the numbers from 0 to 14. In the second, these numbers modulo 3. In the third, write the numbers with modulo 5. What do you notice?

Value	Modulo 3	Modulo 5
0	**0**	**0**
1	**1**	**1**
2	**2**	**2**
3	**0**	**3**
4	**1**	**4**
5	**2**	**0**
6	**0**	**1**
7	**1**	**2**
8	**2**	**3**
9	**0**	**4**
10	**1**	**0**
11	**2**	**1**
12	**0**	**2**
13	**1**	**3**
14	**2**	**4**

I can see that the values repeat in cycles of 3 and 5 respectively, furthermore, if two numbers have the same remainder for mod3 and mod5, then the remainder will be mod15 (or multiples of these values). We can also see that because of this, $\mathbb{Z}_{15} \to \mathbb{Z}_3 \text{x} \mathbb{Z}_5$, that is to say that $f(i) = (i\text{mod}3, i\text{mod}5)$ is bijective.

b. Prove that if p, q are two distinct primes, then for every $(j, k) \in \mathbb{Z}_p \text{x} \mathbb{Z}_q$ there is a single $i \in \mathbb{Z}_{pq}$ such that:

$\text{i} \equiv \text{kmodq}$ and $\text{i} \equiv \text{jmodp}$
Hint: prove that $f : \mathbb{Z}_{pq} \to \mathbb{Z}_p \text{x} \mathbb{Z}_q$ which is defined by $f(i) = (i\text{mod}p, i\text{mod}q)$ and it is injective.

As we know that this is bijective from part a, it is enough to prove it is injective.
Let $\text{a}, \text{b} \in \mathbb{Z}_{\text{pq}}$. Assume f(a) = f(b), so we get:
$(\text{amodp}, \text{amodq}) \equiv (\text{bmodp}, \text{bmodq}) \to (\text{a} \equiv \text{bmodp}) \wedge (\text{a} \equiv \text{bmodq}) \to \text{p}(|\text{a} - \text{b}) \wedge (\text{q}|\text{a} - \text{b}) \to a \equiv \text{bmodpq}$
Since we have $\text{a}, \text{b} \in \mathbb{Z}_{pq}$, we can see that a = b, and our f is 1-1.

c. Prove that the mapping $g : \mathbb{Z}_p \mathrm{x} \mathbb{Z}_q \rightarrow \mathbb{Z}_{pq}$ is the opposite of the mapping $f : \mathbb{Z}_{pq} \rightarrow \mathbb{Z}_p \mathrm{x} \mathbb{Z}_q$ from the previous section:

$\mathrm{g(j,k)} = (\mathrm{j} * \mathrm{q} * (\mathrm{q}^{-1} \mathrm{mod p}) + \mathrm{k} * \mathrm{p} * (\mathrm{p}^{-1} \mathrm{mod q})) \mathrm{mod pq}$

Since we know that f is bijective, it has an inverse function. So we can simply show that $\mathrm{f(g(j,k))} = (\mathrm{j,k})$. Now we can evaluate $\mathrm{y} = \mathrm{g(j,k)} = (\mathrm{j} * \mathrm{q}(\mathrm{q}^{-1} \mathrm{mod p}) + \mathrm{k} * \mathrm{p}(\mathrm{p}^{-1} \mathrm{mod q})$. For some c, we can see that $\mathrm{y} = \mathrm{j} * \mathrm{q}(\mathrm{q}^{-1} \mathrm{mod p}) + \mathrm{k} * \mathrm{p}(\mathrm{p}^{-1} \mathrm{mod q}) + \mathrm{c} * \mathrm{pq}$. We can use the distributive properties to solve then:

$\mathrm{y} \equiv \mathrm{j} * \mathrm{q}(\mathrm{q}^{-1} \mathrm{mod p}) + \mathrm{k} * \mathrm{p}(\mathrm{p}^{-1} \mathrm{mod q}) + \mathrm{c} * \mathrm{pq} \equiv (\mathrm{j} * \mathrm{q}(\mathrm{q}^{-1} \mathrm{mod p})) + (\mathrm{k} * \mathrm{p}(\mathrm{p}^{-1} \mathrm{mod q})) + (\mathrm{c} * \mathrm{pq}) \equiv j + 0 + 0 = j \mathrm{mod} p$

$\mathrm{y} \equiv \mathrm{j} * \mathrm{q}(\mathrm{q}^{-1} \mathrm{mod p}) + \mathrm{k} * \mathrm{p}(\mathrm{p}^{-1} \mathrm{mod q}) + \mathrm{c} * \mathrm{pq} \equiv (\mathrm{j} * \mathrm{q}(\mathrm{q}^{-1} \mathrm{mod p})) + (\mathrm{k} * \mathrm{p}(\mathrm{p}^{-1} \mathrm{mod q})) + (\mathrm{c} * \mathrm{pq}) \equiv 0 + k + 0 = k \mathrm{mod} p$

So we get $\mathrm{y} \equiv \mathrm{j mod p}$,$\mathrm{y} \equiv \mathrm{k mod p}$, and we can see that $\mathrm{f(g(j,k))} = \mathrm{f(y)} = (\mathrm{j,k})$