MATH 3320, HOMEWORK #3 - SOLUTIONS

To ensure that you get full credit, be sure to *show your work* in the problems that require calculations. Very little credit is given for answers without justification. Please write in complete sentences to help us understand what you are doing.

You may collaborate with classmates in solving the problems, including the extra credit problems. If you do so, please list their names on your assignment. However, you should not consult *any* other people (except the instructors or TAs), or use online resources. (Seriously, it's very obvious to us when this occurs, and there are drastic consequences, so don't do it!) If you use results that were not proved in class, please provide your own proof.

1.

(a) (10 points) Determine the two missing digits in the number below such that the number is divisible by 72:

$$2846\_071142\_$$

Solution A number is divisible by 72 if and only if it is divisible by both 8 and 9. Divisibility by 8 holds if and only if the number given by the last three digits is divisible by 8. In the present case, this occurs if and only if the last digit is 4. At this point there is only a single digit left undetermined. Divisibility by 9 holds if and only if the sum of the digits is divisible by 9. The sum of all the other digits (including the 4) is 39, so, given the substition of 4 for the last missing digit, the number is divisible by 9 iff and only if the first missing digit is 6.

The missing digits are 6 and 4 respectively.

(b) (10 points) Determine the last two digits in the decimal representation of 2222^{2222}.

Solution We are trying to determine what 2222^{2222} is mod 100. By the Chinese Remainder Theorem, it suffices to work mod 4 and mod 25. Since 2222 has a factor of 2, our number 2222^{2222} has enormously many factors of 2, so it is congruent to 0 mod 4.

To determine 2222^{2222} mod 25, we use Euler's generalization of Fermat's Little Theorem. Observe that 2222 is relatively prime to 25 and $\phi(25) = 20$, so $2222^{20} \equiv 0 \pmod{25}$. Thus $2222^{2222} \equiv 2222^2 \equiv (-3)^2 \equiv 9 \pmod{25}$.

It follows (either by the formula of the Chinese Remainder Theorem or by inspection) that $2222^{2222} \equiv 84 \pmod{25}$.

2. (10 points) Let n be a positive integer greater than 1, and write ϕ for Euler's phi-function (a.k.a. Euler's totient function). Prove the following identity:

$$\sum_{\substack{1 \le a \le n \\ \gcd(a,n)=1}} a = \frac{n\phi(n)}{2}.$$

In other words, the sum of all positive integers less than or equal to n and relatively prime to n is $\frac{n\phi(n)}{2}$.

Solution Observe that for $n > 1$, $\gcd(n, n) \neq 1$ so we may rewrite the bounds for a as $1 \le a \le n-1$. Suppose a is an integer in this range for which $\gcd(a, n) = 1$. Then $n-a$ certainly also satisfies $1 \le a \le n-1$. But we also know that $\gcd(n-a, n) = \gcd(n-a-n, n) = \gcd(-a, n) = \gcd(a, n) = 1$, so $n - a$ is also one of the integers we are summing.

We could obtain the formula by noting that we can (normally) arrange in this manner the integers we are summing into pairs, but then we would have to deal separately with the case $n = 2$ where $n/2$ is an integer satisfying $\gcd(n/2, 1)$ and thus not actually paired with anything else.

We instead use the fact that $a \mapsto n - a$ is a permutation on the set of integers we are summing (i.e. a bijective map from this set to itself) to obtain that the sum below double-counts each such integer:

$$\sum_{\substack{1\le a\le n-1\\ \gcd(a,n)=1}} [a + (n-a)] = \sum_{\substack{1\le a\le n-1\\ \gcd(a,n)=1}} a + \sum_{\substack{1\le a\le n-1\\ \gcd(a,n)=1}} (n-a) = 2 \sum_{\substack{1\le a\le n-1\\ \gcd(a,n)=1}} a.$$

But the sum on the left-hand side is evidently equal to $n\phi(n)$. It follows that the sum we are interested in evaluates to $n\phi(n)/2$.

3. Let p be an odd prime. Prove the following congruences:

(a) (10 points) $(p-3)! \equiv \frac{p-1}{2} \pmod p$.

Solution Recall that we may divide both sides of a congruence mod p by any integer not a multiple of p and have the sides still congruent. (This is because any integer not a multiple of p has an inverse mod p.) By Wilson's Theorem $(p-1)! \equiv -1 \pmod p$. Now since $p-1$ and $p-2$ are not congruent to 0 mod p (as p is an odd prime), we have

$$(p-3)! = (p-1)!/(p-1)(p-2) \equiv -1/(p-1)(p-2) \equiv (-1)(-1)[(p-1)/2] = (p-1)/2 \pmod p.$$

(Note that -1 is obviously inverse to $p-1$, and that $(p-1)/2$ is inverse to $p-2$ because $(p-2)[(p-1)/2] \equiv (-2)(-1)/2 = 1 \pmod p$.)

(b) (10 points) $\binom{p-1}{k} \equiv (-1)^k \pmod p$ for $k = 0, 1, \ldots, p-1$.

Solution Recall that

$$\binom{p-1}{k} = \frac{(p-1)!}{k!(p-1-k)!}.$$

But modulo p

$$k! \equiv (k-p)\cdots(1-p) = (-1)^k(p-k)\cdots(p-1) = (-1)^k(p-1)!/(p-k-1)!.$$

Plugging in for $k!$, we obtain

$$\binom{p-1}{k} \equiv \frac{(p-1)!}{[(-1)^k(p-1)!/(p-k-1)!]\,(p-1-k)!} = \frac{(p-1)!}{(-1)^k(p-1)!} = \frac{1}{(-1)^k} = (-1)^k.$$

4. Without the help of a computer, solve the following congruences:

(a) (10 points) $x^2 - x + 19 \equiv 0 \pmod{125}$.

Solution: Let $f(x) = x^2 - x + 19$. $125 = 5^3$.

First, consider $f(s_1) \equiv 0 \pmod 5$. We get $s_1 \equiv 3 \pmod 5$.

Second, consider $f(s_2) \equiv 0 \pmod{25}$ and suppose $s_2 = 5t_1 + 3$. Then

$$f'(s_1)t_1 \equiv -f(s_1)/5 \pmod 5$$
$$0 \cdot t_1 \equiv 0 \pmod 5$$

t_1 can be any integer.

Third, consider $f(s_3) \equiv 0 \pmod{125}$, and suppose $s_3 = 25t_2 + s_2$.

$$f'(s_2)t_2 \equiv -f(s_2)/25 \pmod 5$$
$$0 \cdot t_2 \equiv -t_1^2 - t_1 - 1 \pmod 5$$

There is no integer t_1 satisfying this equation. So there is **no solution** to this problem.

(b) (10 points) $x^3 - 2x - 5 \equiv 0 \pmod{432}$.

Solution: Let $f(x) = x^3 - 2x - 5$. $432 = 2^4 \cdot 3^3$. We solve $f(x) \equiv 0 \pmod{2^4}$ and $f(x) \equiv 0 \pmod{3^3}$ respectively, and use Chinese remainder theorem to combine them.

1) $f(x) \equiv 0 \pmod{2}^4$:
First, consider $f(s_1) \equiv 0 \pmod 2$. We get $s_1 \equiv 1 \pmod 2$.
Second, consider $f(s_2) \equiv 0 \pmod 4$. Let $s_2 = 2t_1 + s_1$. We have

$$f'(s_1)t_1 \equiv -f(s_1)/2 \pmod 2$$

$$t_1 \equiv 1 \pmod 2$$

Third, consider $f(s_3) \equiv 0 \pmod 8$. Let $s_3 = 4t_2 + s_2 = 4t_2 + 3$.

$$f'(s_2)t_2 \equiv -f(s_2)/4 \pmod 2$$

$$t_2 \equiv 0 \pmod 2$$

Fourth, consider $f(s_4) \equiv 0 \pmod 1)6$. Let $s_4 = 8t_3 + s_3 = 8t_3 + 3$.

$$f'(s_3)t_3 \equiv -f(s_3)/8 \pmod 2$$

$$t_3 \equiv 0 \pmod 2$$

The solution of $f(x) \equiv 0 \pmod 1)6$ is $x \equiv 3 \pmod 1)6$.

2) $f(x) \equiv 0 \pmod 3)^3$:
First, consider $f(s_1) \equiv 0 \pmod 3$. The solution is $s_1 \equiv 1 \pmod 3$.
Second, consider $f(s_2) \equiv 0 \pmod 9$. Let $s_2 = 3t_1 + s_1$.

$$f'(s_1)t_1 \equiv -f(s_1)/3 \pmod 3$$

$$t_1 \equiv 2 \pmod 3$$

Third, consider $f(s_3) \equiv 0 \pmod 2)7$. Let $s_3 = 9t_2 + s_2 = 9t_2 + 7$.

$$f'(s_2)t_2 \equiv -f(s_2)/9 \pmod 3$$

$$t_2 \equiv 0 \pmod 3$$

The solution of $f(x) \equiv 0 \pmod 2)7$ is $x \equiv 7 \pmod 2)7$.

Use Chinese remainder theorem, we get $f(x) \equiv 0 \pmod 4)32$ when $x \equiv 115 \pmod 4)32$.

Comment: the solution should be a class of integers instead of a single number.

The slide section has an extra sample on how to solve such equations.

You may use a computer to check your solutions. Below is sample code in `SAGE` that solves the congruences in part (a):

```
R.<x> = PolynomialRing(Integers(125)
f = x^2 - x + 19
f.roots(multiplicities=False)
```

5.

(a) (10 points) Let n be a fixed positive integer. Prove that there are only finitely many integers m such that $\phi(m) = n$.

Solution: Suppose $m = p_1^{a_1} \cdots p_k^{a_k}$ for distinct prime numbers $p_1, \cdots, p_k$. Then

$$n = \phi(m) = \Pi_{i=1}^{k}(p_i^{a_i - 1}(p_i - 1))$$

For each i, we have $p_i \leq n+1$ and $a_i \leq \log_{p_i} n+1$. There are finite many p_i and a_i satisfying the inequalities. Thus m also has finite many ways of combination.

(b) (10 points) Find all positive integers m such that $\phi(m)$ divides m. (Hint: First show that the smallest prime factor of m must be 2.)

Solution: When $m > 1$, suppose $m = 2^a$. Then $\phi(m) = 2^{a-1}(2-1)|2^a = m$, satisfying the condition.

If m has odd prime factor, say p. Then

$$p - 1|\phi(m)|m$$

Because $p > 2$ is prime, $p-1$ is even. So m must be even. Suppose $m = 2^{a_0}\Pi_{i=1}^{k} p_i^{a_i}$ for distinct prime numbers $2 < p_1 < \cdots < p_k$.

$$\phi(m) = 2^{a_0-1}\Pi_{i=1}^{k}(p_i^{a_i-1}(p_i-1))$$

$$m/\phi(m) = \frac{2\Pi_{i=1}^{k} p_i}{\Pi_{i=1}^{k}(p_i-1)} \in Z$$

Because $\gcd(p_1-1, p_j) = 1$ for all $j = 1, \cdots, k$, $p_1 - 1$ can only be equal to 2, that is $p_1 = 3$. If m has prime factor other than 2 and 3, then we have

$$m/\phi(m) = \frac{\Pi_{i=1}^{k} p_i}{\Pi_{i=2}^{k}(p_i-1)} \in Z$$

Notice the denominator is even but numerator is odd, m cannot have prime factors other than 2 and 3. Therefore, m should be either 2^a or $2^a 3^b$. For the second case, $a \geq 1$.

6. (Extra Credit) In geometry, a *star polygon* is a polygon that can be constructed as follows:

Step 1. Take $n \geq 3$ regularly spaced points $P_1, P_2, \ldots, P_n$ on a circle, numbered clockwise.
Step 2. Choose a positive integer $m < n$ and connect P_i and P_{i+m} by a line segment for each $i = 1, 2, \ldots, n$. (We set $P_{n+k} = P_k$ for any integer k.)

We denote the resulting polygon using the symbol $\{n/m\}$. The points $P_1, P_2, \ldots, P_n$ chosen in Step 1 are called *vertices* and the line segments $\overline{P_i P_{i+m}}$ drawn in Step 2 are called *edges*.

If $m = 1$, we obtain the regular polygons, which are familiar from our geometry classes. Star polygons often show up in art and some have their own special names. For example, $\{5/2\}$ is called a pentagram and $\{6/2\}$ is often referred to as the Star of David.

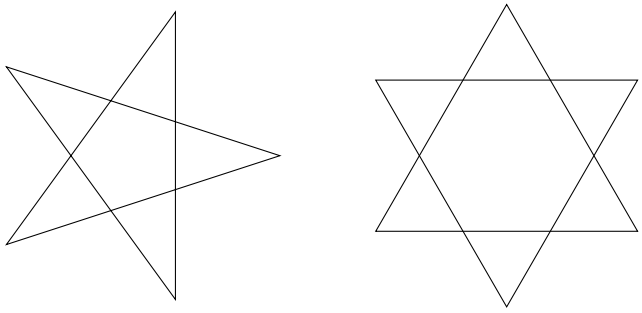

FIGURE 1. The star polygons $\{5/2\}$ and $\{6/2\}$.

A star polygon is said to be *proper* if every vertex can be reached from a given vertex by travelling along the edges. For example, $\{\frac{5}{2}\}$ is proper, but $\{\frac{6}{2}\}$ is not.

For (10 points), determine the number of distinct proper star polygons with fixed vertices $P_1, P_2, \ldots, P_n$. Your answer may be given in terms of the Euler ϕ-function.

Solution: We prove $\{n/m\}$ is proper if and only if $\gcd(n, m) = 1$:

- If $\gcd(n, m) = d > 1$, we start from P_i. After travelling k steps, we reach P_j, where $j \equiv i + mk \pmod{n}$. Because $d|n, d|m$, we have

$$j \equiv i + mk \equiv i \pmod{d}.$$

Then starting from P_i, we can't reach those vertices P_j where $j \not\equiv i \pmod{d}$.

- If $\gcd(n, m) = 1$, starting from any vertex P_i, we should reach all n points in first n steps. Otherwise, by pigeonhole principle, there exists a vertex P_j reached at least twice in the first n steps. In this case, suppose we reached P_j at step k_1 and k_2, where $1 \leq k_1 < k_2 \leq n$. So

$$j + (k_2 - k_1)m \equiv j \pmod{n}.$$
$$(k_2 - k_1)m \equiv 0 \pmod{n}.$$

  Because $\gcd(m, n) = 1$, we have $k_2 - k_1 \equiv 0 \pmod{n}$, which contradicts with $0 < k_2 - k_1 < n$. So If $\gcd(n, m) = 1$, all vertices can be reached starting from any vertex.

$\{n/m_1\}$ and $\{n/m_2\}$ generate the same star polygon if and only if $m_1 \equiv m_2 \pmod{n}$ or $m_1 \equiv -m_2 \pmod{n}$. Thus, there are $\phi(\mathbf{n})/\mathbf{2}$ distinct proper star polygons.