MATH 304: MIDTERM EXAM SOLUTIONS

[The problems are each worth five points, except for problem 8, which is worth 8 points. Thus there are 43 possible points.]

1. Use the Euclidean algorithm to find the greatest common divisor of 7462 and 2464.

$$\begin{aligned} 7462 &= 3 \cdot 2464 + 70 \\ 2464 &= 35 \cdot 70 + 14 \\ 70 &= 5 \cdot 14 + 0 \end{aligned}$$

   The last nonzero remainder is the greatest common divisor of the initial pair, so $\mathrm{GCD}(7462, 2462) = 14$.

2. How many of the integers between 0 and 600 are relatively prime to 600?

   By definition, the Euler ϕ-function of n is the number of numbers between 0 and n that are relatively prime to n. Using the fact that $\phi(m \cdot n) = \phi(m)\phi(n)$ whenever $\mathrm{GCD}(m, n) = 1$, and that for prime powers $\phi(p^e) = p^e - p^{e-1}$, we compute that:

$$\begin{aligned} \phi(600) = \phi(2^3 \cdot 3 \cdot 5^2) &= \phi(2^3)\phi(3)\phi(5^2) \\ &= (2^3 - 2^2)(3 - 3^0)(5^2 - 5) = 4 \cdot 2 \cdot 20 = 160. \end{aligned}$$

   Therefore there are 160 numbers between 0 and 600 that are relatively prime to 600.

3. Find the remainder when 3^{39} is divided by 21.

   By Fermat's little theorem with $p = 7$, we have the congruence:

$$3^{39} = 3^{6 \cdot 6 + 3} = (3^6)^6 \cdot 3^3 \equiv 1^6 \cdot 3^3 \equiv 6 \pmod 7.$$

   On the other hand, 3 clearly divides the difference $3^{39} - 6$ as well. Therefore the product $21 = 3 \cdot 7$ also divides the difference, so we have:

$$3^{39} \equiv 6 \pmod{21}.$$

   It follows that when you divide 3^{39} by 21 the remainder is 6.

4. Suppose that $a^{24} \equiv 1 \pmod{19}$. What are the possible orders of a modulo 19?

   By the order divisibility property, if $a^k \equiv 1 \pmod{19}$, then the order of a modulo 19 must divide k. In our situation where $k = 24$, this means that the order of a must be one of the following numbers:

$$e_p(a) = 1, 2, 3, 4, 6, 12, 24.$$

On the other hand, by Fermat's little theorem $a^{18} \equiv 1 \pmod{19}$. Thus by the order divisibility property again, the order of a modulo 19 must divide 18, and thus must be one of the following numbers:

$$e_p(a) = 1, 2, 3, 6, 9, 18.$$

The numbers that occur in both lists are the possible values for the order of a modulo 19:

$$e_p(a) = 1, 2, 3, 6.$$

5. Do there exist integer solutions x, y to the equation $36x + 56y = 12$? Explain your reasoning.

   Recall that the smallest positive integer that can be written as a linear combination $ax + by$ of a and b is the greatest common divisor $\mathrm{GCD}(a, b)$.

   In our situation, we have $\mathrm{GCD}(36, 56) = 4$, so there exist integers x_0 and y_0 such that

   $$36x_0 + 56y_0 = 4.$$

   Multiplying by 3, we see that $(x, y) = (3x_0, 3y_0)$ is an integer solution to the given equation:

   $$36(3x_0) + 56(3y_0) = 3 \cdot 4 = 12.$$

   (In fact, $(x_0, y_0) = (11, -7)$ are solutions to the first equation, so $(x, y) = (33, -21)$ are solutions to the desired equation. But you DON'T need to find a solution to answer the given question!)

6. Let p be a prime number and let x and y be integers. Prove that

   $$(x + y)^p \equiv x^p + y^p \pmod{p}.$$

   Let z be an integer. If p divides z, then $z^p \equiv z \pmod{p}$ is true because p divides both sides. On the other hand, if p does not divide z, then $z^p \equiv z \pmod{p}$ holds by Fermat's little theorem. This shows that $z^p \equiv z \pmod{p}$ is is always true.

   Applying this fact in the cases $z = x + y$, $z = x$ and $z = y$, we see that:

   $$(x + y)^p \equiv x + y \equiv x^p + y^p \pmod{p}.$$

   Remark: we proved this fact (affectionately called the "freshman's dream" because the equation $(x + y)^n = x^n + y^n$ is a common bit of wishful thinking among the young) using Fermat's little theorem. But in fact, we could have done things in the opposite order! That is, there is a proof that does not rely on Fermat's little theorem, and then we can prove Fermat's little theorem using this fact. Here's how this goes.

The binomial coefficient $\binom{n}{k}$ (pronounced "n choose k") is the number of ways of choosing k (unordered) objects from a collection of n objects. One can show that:

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

(So in particular this fraction is an integer!) Consider the expression $(x+y)^n$. In the final product, the coefficient of y^k is exactly the number of ways to choose k of the n different terms $(x+y)$ to take a factor of y from. It follows that:

$$\begin{aligned}(x+y)^n &= x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots \binom{n}{n-2}x^2y^{n-2} + \binom{n}{n-1}xy^{n-1} + y^n \\ &= \sum_{i=0}^{n} \binom{n}{i} x^{n-i}y^i.\end{aligned}$$

(Notice that by the symmetry of this expression in x and y, this argument shows that $\binom{n}{k} = \binom{n}{n-k}$, a fact which is also apparent from the formula $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.)

Now, we wish to use this formula in the case where $n = p$ is a prime number. The key fact is that p divides $\binom{p}{k}$ when $1 \leq k \leq p-1$. To prove this, notice that p does not divide either $k!$ or $(p-k)!$, since each term in these products is less than p and hence relatively prime to p. It follows that in the fraction

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

there is no factor of p in the denominator. Since there is a factor of p in the numerator, it follows that p divides the whole expression. This proves that p divides $\binom{p}{k}$ when $1 \leq k \leq p-1$.

It follows that in the binomial expansion

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i}y^i,$$

all terms are divisible by p except for the summands corresponding to $i = 0$ and $i = p$. Therefore, $(x+y)^p \equiv x^p + y^p \pmod{p}$ as claimed.

Here is the proof of Fermat's little theorem starting from the "freshman's dream". We will prove that $a^p \equiv a \pmod{p}$ for all positive integers a by induction on a. It is clearly true for $a = 1$. Assume inductively that the statement holds for the integer $a-1$. By the "freshman's dream",

$$a^p = ((a-1)+1)^p \equiv (a-1)^p + 1^p = (a-1)^p + 1 \pmod{p}.$$

On the other hand, $(a-1)^p \equiv a-1$ by the inductive hypothesis. It follows that

$$a^p \equiv (a-1) + 1 = a \pmod{p}.$$

Having proved the general statement, we can derive Fermat's little theorem by taking a relatively prime to p. In this case, we may divide p from both sides of the congruence, yielding $a^{p-1} \equiv 1 \pmod{p}$. Thus concludes our alternative proof of Fermat's little theorem.

7. Let p be an odd prime number and suppose that g and g' are both primitive roots modulo p. Prove that their product gg' is not a primitive root modulo p.

   Since p is odd, the fraction $\frac{p-1}{2}$ is an integer. I claim that for a primitive root g,

   $$g^{(p-1)/2} \equiv -1 \pmod{p}.$$

   To see this, write $x = g^{(p-1)/2}$, and notice that

   $$x^2 = \left(g^{(p-1)/2}\right)^2 = g^{(p-1)} \equiv 1 \pmod{p}.$$

   Therefore, $x \equiv \pm 1 \pmod{p}$. Since g is a primitive root, it cannot be the case that $x = g^{(p-1)/2} \equiv 1 \pmod{p}$. It follows that $g^{(p-1)/2} \equiv -1 \pmod{p}$.

   Applying this argument for both of the primitive roots g and g', we see that:

   $$(gg')^{(p-1)/2} = g^{(p-1)/2} g'^{(p-1)/2} \equiv (-1) \cdot (-1) = 1 \pmod{p}.$$

   This is an instance of a congruence $g^k \equiv 1 \pmod{p}$ with $k < p-1$, which shows that gg' is not a primitive root.

8. (a) Let p be a prime number and let g be a primitive root mod p. Show that

   $$(p-1)! \equiv g^{p(p-1)/2} \pmod{p}.$$

   Since g is a primitive root, the residue classes

   $$g, g^2, g^3, \ldots, g^{p-1} \pmod{p}$$

   are all distinct. Hence the above list of residue classes is the same as the list

   $$1, 2, \ldots, p-1 \pmod{p},$$

   but in a different order. Taking the product of all residue classes in the list, we see that:

   $$(p-1)! \equiv g \cdot g^2 \cdot \cdots \cdot g^{p-1} = g^{1+2+3+\cdots+(p-1)} \pmod{p}.$$

   Using the identity

   $$1 + 2 + 3 + \cdots + k = \sum_{i=1}^{k} i = \frac{(k+1)k}{2}$$

with $k = p - 1$, we conclude that:

$$(p-1)! \equiv g^{1+2+3+\cdots+(p-1)} = g^{\frac{p(p-1)}{2}} \pmod{p},$$

as desired.

(b) Use part (a) to deduce that

$$(p-1)! \equiv -1 \pmod{p}.$$

[Note: to receive credit on this problem, you must prove the result using part (a). It is not fair to just quote the HW where you proved this in a different way!]

If $p = 2$, then

$$(p-1)! = 1! = 1 \equiv -1 \pmod{2},$$

so the congruence holds.

Now assume that p is odd. By the proof given in problem 7, we know that $g^{(p-1)/2} \equiv -1 \pmod{p}$. Applying part (a), we have:

$$(p-1)! \equiv g^{\frac{p(p-1)}{2}} = \left(g^{(p-1)/2}\right)^p \equiv (-1)^p \pmod{p}.$$

We know that $(-1)^p = -1$ because p is odd. Therefore, $(p-1)! \equiv -1 \pmod{p}$.