

18.781: MIDTERM 1

MARCH 7, 2003

Instructions: To receive credit for a solution, your answer must be explained fully in complete sentences. Correct answers without proper explanation will receive no credit.

No notes, books, or calculators are allowed.

Each question is worth ten (10) points.

(1) Compute the greatest common divisor g of 423 and 198. Then find integers x and y so that $g = 423x + 198y$.

Answer. Using the Euclidian algorithm

$$423 = 2(198) + 27$$

$$198 = 7(27) + 9$$

$$27 = 3(9),$$

so $g = 9$. To find x and y , write

$$9 = 198 - 7(27) = 198 - 7(423 - 2 * 198) = 15(198) - 7(423),$$

so take $x = -7$ and $y = 15$.

(2) Write down the definition of a reduced residue system modulo an integer m . Then show that any two reduced residue systems modulo m have the same number of elements.

Answer. A reduced residue system modulo m is a set of integers $\{r_1, \dots, r_s\}$ prime to m so that for any integer x prime to m there exists a unique i in $[1, s]$ with

$$x \equiv r_i \pmod{m}.$$

Note that the uniqueness of i in the above implies that r_i is not congruent to r_j for $j \neq i$.

If $\{r'_1, \dots, r'_{s'}\}$ is a second reduced residue system, define a set map

$$\{r_1, \dots, r_s\} \longrightarrow \{r'_1, \dots, r'_{s'}\}$$

by sending r_i to the unique r'_j for which $r_i \equiv r'_j \pmod{m}$. If r_i and r_j map to the same element under the above map, then $r_i \equiv r_j \pmod{m}$, and so $i = j$ and the map is injective. That the map is surjective follows from the definition of reduced residue system given above.

(3) Show that -1 is not a square modulo a prime p if $p \equiv 3 \pmod{4}$.

Answer. Suppose by contradiction that there exists an integer x with $x^2 \equiv -1 \pmod{p}$. Raising both sides of the equation to the $(p-1)/2$ -th power and noting that $(p-1)/2$ is odd since $p \equiv 3 \pmod{4}$, we find that

$$x^{p-1} \equiv -1 \pmod{p}.$$

Now since $(p, x^2) = 1$, we have $(x, p) = 1$ and so by Euler's theorem $x^{p-1} \equiv 1 \pmod{p}$. We therefore find that

$$1 \equiv -1 \pmod{p}$$

which is a contradiction.

(4) Let p be a prime number. Show that the numerator of

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

is divisible by p (Hint: Clear denominators).

Answer. It was stated in class that the assumption that $p > 2$ should be added to the problem.

Let us first note that if a/b is any rational number with $(a, b) = 1$ and if c is any integer prime to p , then $p|ca$ if and only if p divides the numerator of the rational number $(ca)/b$. Therefore, it suffices to show that $(p-1)!$ times the above number is divisible by p .

Now if we multiply the above number by $(p-1)!$, we get

$$(1) \quad 1 + \sum_{j=2}^{p-1} \frac{(p-1)!}{j}.$$

The key point is that the set $\{0, 1, \frac{(p-1)!}{j}\}$, where $j = 2, \dots, p-1$, is a complete residue system modulo p . To prove this it suffices to show $\frac{(p-1)!}{j}$ is not congruent to $\frac{(p-1)!}{j'}$ modulo p for $j \neq j'$. But this is clear, for by Wilson's theorem the number $\frac{(p-1)!}{j}$ defines the unique congruence class modulo p of integers r for which

$$jr \equiv -1 \pmod{p}.$$

Thus $\{0, 1, \frac{(p-1)!}{j}\}$ is a complete residue system modulo p . It follows that each number in this set is congruent to a unique number in $\{0, 1, 2, \dots, p-1\}$, and hence the sum (1) is congruent to

$$1 + 2 + 3 + \cdots + (p-1)$$

modulo p . This sum is in turn equal to $p(p-1)/2$, and since $(p-1)/2$ is an integer if $p > 2$, this implies that the sum is congruent to 0 modulo p .

(5) Show that if $n \geq 1$, then

$$\sum_{k=0}^n (-1)^k \binom{n}{k} = 0.$$

Answer. By the binomial theorem

$$0 = (1 + (-1))^n = \sum_{k=0}^n \binom{n}{k} (-1)^k.$$