MATH 115, SUMMER 2012
MIDTERM EXAM
WEDNESDAY, JULY 18TH

JAMES MCIVOR

The exam is out of 180 points. You have the full class time (1 hour, fifty minutes) to complete it. No calculators or cheat sheets are allowed, and do not use your cellphone, etc... You must explain your work clearly in complete English sentences for full credit. The letter p always stands for a prime number.

(1) (5 points each) True or False. Give a very brief reason for your answers.

(a) Let $m, c > 0$. If $a \equiv b \mod mc$ then $a \equiv b \mod m$.
True: If $mc|(a-b)$ then also $m|(a-b)$.

(b) Let $m, c > 0$. If $a \equiv b \mod m$ then $a \equiv b \mod mc$.
False: For example, 2 is congruent to 7 mod 5 but not mod 10.

(c) If $m = pq$, with p, q distinct primes, then $\phi(m) \equiv 1 - p - q \mod m$.
True: $\phi(m) = \phi(p)\phi(q) = (p-1)(q-1) = m - p - q + 1 \equiv -p - q + 1 \mod m$.

(d) If the ring $\mathbb{Z}/m$ contains zerodivisors, then m is composite.
True: Zerodivisors in the ring $\mathbb{Z}/m$ are nonzero integers less than m which are not prime to m, and there are none of these if m is prime.

(e) If $a|c$ and $b|c$, then $ab|c$.
False: Take $a = b = c = 2$ for a counterexample.

(f) If $p \equiv 1 \mod 4$, then the congruence $x^2 \equiv -1 \mod p$ has a solution.
True: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, which is 1 if $p \equiv 1 \mod 4$.

(g) If $(ab, p) = 1$, then

$$\frac{(ab)^{p-1} - 1}{p} \equiv \frac{a^{p-1} - 1}{p} + \frac{b^{p-1} - 1}{p} \mod p$$

True: $(ab, p) = 1$ implies that also $(a, p) = (b, p) = 1$. Fermat's Little Theorem says $a^{p-1} \equiv 1 \mod p$ and $b^{p-1} \equiv 1 \mod p$. So there are integers k, m with $a^{p-1} - 1 = kp$, $b^{p-1} = mp$. Then

$$(ab)^{p-1} = (kp+1)(mp+1) = kmp^2 + (k+m)p + 1,$$

so

$$\frac{(ab)^{p-1} - 1}{p} = kmp + k + m \equiv k + m = \frac{a^{p-1} - 1}{p} + \frac{b^{p-1} - 1}{p} \mod p$$

(h) 4 is a primitive root mod 5.
False: $4^2 = 16 \equiv 1 \mod 5$.

(2) (15 points) Find the smallest positive integer a such that $3^{52} \equiv a \mod 40$.
Solution: $a = 1$

(3) (10 points) Find the gcd of 234 and 108 and express it as a $\mathbb{Z}$-linear combination of 234 and 108.

Solution: $(234, 108) = 18$; $18 = 1 \cdot 234 - 2 \cdot 108$.

(4) (10 points) Explain why the equation

$$72x - 42y = 112$$

has no solutions in integers x, y.

Solution: The gcd of 72 and -42 is 6. Any $\mathbb{Z}$-linear combination of these two must be a multiple of 6, but 112 is not.

(5) (20 points) Solve the following system of congruences for x:

$$\begin{aligned} x &\equiv 1 \mod 4 \\ x &\equiv 3 \mod 5 \\ x &\equiv 5 \mod 7 \end{aligned}$$

Be sure to describe *all* solutions.

Solution: $x \equiv 33 \mod 120$.

(6) (15 points) Find *all* solutions, if any, to the congruence

$$12x \equiv 18 \mod 30$$

Solution: Since the gcd of 12 and 30 is 6, and this divides 18, the congruence is equivalent to

$$2x \equiv 3 \mod 5$$

the inverse of 2 mod 5 is 3, so multplying through by 3 gives

$$x \equiv 4 \mod 5$$

(7) (5 points) Compute $\phi(140)$.

Solution: $\phi(140) = \phi(4)\phi(5)\phi(7) = 2 \cdot 4 \cdot 6 = 48$.

(8) (15 points) Solve the congruence

$$x^2 + x \equiv 0 \mod 27$$

Solution: Two roots mod 3, 0 and 2. Both are nonsingular, so there will be exactly two roots mod 27. The root zero mod 3 clearly lifts to 0 mod 27. For the other root, set $a = a_1 = 2$, so $f'(a) = 2$ and $f'(a)^{-1} = 2 \mod 3$.

$$\begin{aligned} a_2 &= a_1 - f(a_1) \cdot = 2 - 6 \cdot 2 = -10 \equiv -1 \mod 9 \\ a_3 &= a_2 - f(a_2) \cdot 3 = -1 - 0 \cdot 2 = -1 \mod 27 \end{aligned}$$

You may also have simply observed that -1 and zero are roots for any modulus, and used the fact that the congruence has at most two roots, so there are no others. But if you did this shortcut, you had to justify why 0 and -1 are the only roots.

(9) (20 points) Determine whether the following congruences have a solution. Justify your answer carefully.

(a) $x^2 \equiv 101 \mod 61$

(b) $x^2 + 90 \equiv 0 \mod 19$

Solution: It's enough to compute the Legendre symbol for each case. For (a), we have

$$\left(\frac{101}{61}\right) = \left(\frac{40}{61}\right) = \left(\frac{2}{61}\right)^3 \left(\frac{5}{61}\right) = (-1)^3 \left(\frac{61}{5}\right) (-1)^{\frac{60}{2}\frac{4}{2}} = -\left(\frac{1}{5}\right) = -1,$$

so the congruence (a) has no solution.

The congruence in (b) is equivalent to $x^2 \equiv -90 \mod 19$, for which we compute

$$\left(\frac{-90}{19}\right) = \left(\frac{-1}{19}\right)\left(\frac{2}{19}\right)\left(\frac{3}{19}\right)^2\left(\frac{5}{19}\right) = (-1)(-1)(1)\left(\frac{19}{5}\right)(-1)^{\frac{18}{2}\frac{4}{2}} = \left(\frac{4}{5}\right),$$

which is 1, so this congruence does have a solution.

(10) (15 points) Prove that the congruence

$$(x^2-2)(x^2-17)(x^2-34) \equiv 0 \mod p$$

has a solution for every odd prime p.

Solution: This has a solution if at least one of the three congruences

$$x^2 \equiv 2 \mod p$$
$$x^2 \equiv 17 \mod p$$
$$x^2 \equiv 34 \mod p$$

The first one has a solution iff $p \equiv \pm 1 \mod 8$. So we might as well assume that $p \equiv \pm 3 \mod 8$. In this case we have $\left(\frac{2}{p}\right) = -1$, and also $p \neq 17$, so $\left(\frac{p}{17}\right) \neq 0$. So

$$\left(\frac{34}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{17}{p}\right) = (-1)\left(\frac{17}{p}\right)$$

so if the second congruence does not have a solution, then the third one does, and vice versa.

(11) (15 points) Let p be a odd prime, and q a prime factor of $2^p - 1$. Prove that the order of 2 mod q is p, and that therefore $p|(q-1)$.

Solution: Let the order of 2 mod q be h. Since $q|2^p - 1$, we have $2^p \equiv 1 \mod q$, and therefore $h|p$. Since p is prime, $h = 1$ or p. But h cannot be 1 since the only element of order 1 is 1 itself. So $h = p$, proving the first claim. For the second part, since $q|2^p - 1$, which is odd, q itself is odd, so we have by Fermat's Little Theorem that

$$2^{q-1} \equiv 1 \mod q,$$

and it follows that $p|q-1$, since p is the order of 2.