

MATH 230
STUDY GUIDE FOR MIDTERM 2

(1) Make the following calculations in modular arithmetic. Your answer should be an integer in the range $0, 1, \dots, m - 1$, where m is the modulus.

(a) $2^{138} \pmod{213}$

$213 = 3 \cdot 71$, so $\phi(213) = 2 \cdot 70 = 140$. Euler's Theorem says that $2^{140} \equiv 1 \pmod{213}$, so

$$2^{138} \equiv \frac{2^{140}}{2^2} \equiv \frac{1}{4} \equiv \frac{-212}{4} \equiv -53 \equiv \boxed{160} \pmod{213}.$$

(b) $3^{173} \pmod{215}$

$215 = 5 \cdot 43$, so $\phi(215) = 4 \cdot 42 = 168$. Euler's Theorem says that $3^{168} \equiv 1 \pmod{215}$, so

$$3^{173} \equiv 3^{168} \cdot 3^5 \equiv 3^5 \equiv 243 \equiv \boxed{28} \pmod{215}.$$

(c) $5^{216} \pmod{217}$

$217 = 7 \cdot 31$, so $\phi(217) = 6 \cdot 30 = 180$. Euler's Theorem says that $5^{180} \equiv 1 \pmod{217}$, so

$$5^{216} \equiv 5^{180} \cdot 5^{36} \equiv 5^{36}.$$

Now we compute

$$5^4 = 625 \equiv -26 \pmod{217}$$

$$5^8 \equiv (-26)^2 \equiv 676 \equiv 25 \pmod{217}$$

Since $5^8 \equiv 5^2 \pmod{217}$, we must have $5^6 \equiv 1 \pmod{217}$, so

$$5^{36} \equiv (5^6)^6 \equiv 1^6 \equiv \boxed{1} \pmod{217}.$$

Since $5^{216} \equiv 1 \pmod{217}$, but 217 is composite, 217 is called a *pseudoprime* to base 5.

(2) Determine which of the following congruences are solvable:

(a) $x^2 \equiv 3 \pmod{17}$

$$\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

so this congruence is not solvable.

(b) $x^2 \equiv 3 \pmod{19}$

$$\left(\frac{3}{19}\right) = -\left(\frac{19}{3}\right) = -\left(\frac{1}{3}\right) = -1,$$

so this congruence is not solvable.

(c) $x^2 \equiv 5 \pmod{19}$

$$\left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = 1,$$

so this congruence is solvable.

(d) $x^2 \equiv 3 \pmod{323}$

Note that $323 = 17 \cdot 19$. By the Chinese Remainder Theorem, this congruence is equivalent to the pair of congruences

$$x^2 \equiv 3 \pmod{17}; \quad x^2 \equiv 3 \pmod{19}.$$

Neither of these is solvable, as we saw in parts (a) and (b), so this congruence is also not solvable.

(e) $x^3 \equiv 5 \pmod{19}$

We can determine the solvability of this congruence by making a list of all of the cubes mod 19:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
x^3	0	1	8	8	7	11	7	1	18	7	12	1	18	12	8	12	11	11	18

Since 5 does not appear among the list of cubes, we may conclude that this congruence is not solvable.

Alternatively, suppose $x^3 \equiv 5 \pmod{18}$. Then

$$x^{18} \equiv (x^3)^6 \equiv 5^6 \equiv 5^2 \cdot 5^2 \cdot 5^2 \equiv 6 \cdot 6 \cdot 6 \equiv 6 \cdot 36 \equiv 6(-2) \equiv -12 \equiv 7 \pmod{19}.$$

This contradiction of Fermat's Theorem shows that no such x could exist.

(f) $x^5 \equiv 5 \pmod{19}$

Since $\gcd(5, 18) = 1$, $x^5 \equiv a \pmod{19}$ is solvable for all values of a .

(g) $x^9 \equiv 5 \pmod{19}$

$$x^9 \equiv \left(\frac{x}{19}\right) \equiv \pm 1 \pmod{19},$$

so this congruence is not solvable.

(3) Calculate the following Legendre symbols:

(a) $\left(\frac{22}{97}\right)$

$$\left(\frac{22}{97}\right) = \left(\frac{2}{97}\right) \left(\frac{11}{97}\right) = \left(\frac{11}{97}\right) = \left(\frac{97}{11}\right) = \left(\frac{9}{11}\right) = \boxed{1}.$$

(b) $\left(\frac{35}{97}\right)$

$$\left(\frac{35}{97}\right) = \left(\frac{5}{97}\right) \left(\frac{7}{97}\right) = \left(\frac{97}{5}\right) \left(\frac{97}{7}\right) = \left(\frac{2}{5}\right) \left(\frac{-1}{7}\right) = (-1)(-1) = \boxed{1}.$$

Alternatively, using Jacobi symbols,

$$\left(\frac{35}{97}\right) = \left(\frac{97}{35}\right) = \left(\frac{-8}{35}\right) = \left(\frac{-1}{35}\right) \left(\frac{2}{35}\right) = (-1)(-1) = \boxed{1}.$$

(c) $\left(\frac{-56}{97}\right)$

$$\begin{aligned} \left(\frac{-56}{97}\right) &= \left(\frac{41}{97}\right) = \left(\frac{97}{41}\right) = \left(\frac{15}{41}\right) = \left(\frac{3}{41}\right) \left(\frac{5}{41}\right) \\ &= \left(\frac{41}{3}\right) \left(\frac{41}{5}\right) = \left(\frac{2}{3}\right) \left(\frac{1}{5}\right) = (-1)(1) = \boxed{-1}. \end{aligned}$$

We could also have computed $\left(\frac{15}{41}\right)$ using Jacobi symbols as

$$\left(\frac{15}{41}\right) = \left(\frac{41}{15}\right) = \left(\frac{-4}{15}\right) = \left(\frac{-1}{15}\right) = \boxed{-1}.$$

Alternatively,

$$\left(\frac{-56}{97}\right) = \left(\frac{-1}{97}\right) \left(\frac{8}{97}\right) \left(\frac{7}{97}\right) = (1)(1) \left(\frac{7}{97}\right) = \left(\frac{97}{7}\right) = \left(\frac{-1}{7}\right) = \boxed{-1}.$$

(4) Solve the following congruences:

(a) $x^2 \equiv 5 \pmod{19}$

The simplest way to solve this congruence is to make a table of squares mod 19:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
x^2	0	1	4	9	16	6	17	11	7	5	5	7	11	17	6	16	9	4	1

So we see that the solutions are $\boxed{\pm 9 \pmod{19}}$.

Alternatively, $5^9 \equiv \left(\frac{5}{19}\right) \equiv 1 \pmod{19}$, so $5^{10} \equiv 5 \pmod{19}$. It follows that 5^5 is a square root of 5 mod 19, and

$$5^5 \equiv 5^2 \cdot 5^2 \cdot 5 \equiv 6 \cdot 6 \cdot 5 \equiv 36 \cdot 5 \equiv 5(-2) \equiv -10 \equiv 9 \pmod{19},$$

which shows that the solutions are $\boxed{\pm 9 \pmod{19}}$.

(b) $x^5 \equiv 2 \pmod{19}$

We must find $x \equiv 2^{1/5} \pmod{19}$. By Fermat's Theorem, $2^a \equiv 2^b \pmod{19}$ if $a \equiv b \pmod{18}$, so we compute $\frac{1}{5} \pmod{18}$:

$$\frac{1}{5} \equiv \frac{-35}{5} \equiv -7 \equiv 11 \pmod{18}.$$

Thus

$$2^{1/5} \equiv 2^{11} \equiv 2^4 \cdot 2^4 \cdot 2^3 \equiv (-3)(-3)(8) \equiv 72 \equiv \boxed{15 \pmod{19}}.$$

(c) $2^x \equiv 5 \pmod{19}$

Again, the most straightforward way to solve this problem is to make a table of the powers of 2 mod 19:

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^x	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

Thus $2^{16} \equiv 5 \pmod{19}$. Since the powers of 2 repeat in cycles of 18, by Fermat's Theorem, we see that the solution is $x \equiv \boxed{16 \pmod{18}}$.

Alternatively, since

$$5 \equiv \frac{1}{4} \equiv 2^{-2} \pmod{19},$$

we see that the solution is $x \equiv -2 \equiv \boxed{16 \pmod{18}}$.

- (5) (a) Find a primitive root mod 31.
2 is not a primitive root, since $2^5 = 32 \equiv 1 \pmod{31}$. Let's try 3.

$$3^{15} \equiv \left(\frac{3}{31}\right) \equiv -\left(\frac{31}{3}\right) \equiv -\left(\frac{1}{3}\right) \equiv -1 \pmod{31}$$

$$3^{10} \equiv 3^5 \cdot 3^5 \equiv 243 \cdot 243 \equiv (-5)(-5) \equiv 25 \pmod{31}$$

$$3^6 \equiv (3^3)^2 \equiv (-4)^2 \equiv 16 \pmod{31}$$

The order of 3 must be a divisor of 30, but by the above calculations it is not a divisor of 15, 10, or 6. The only such number is 30, so 3 is a primitive root mod 31.

- (b) Find all values of x such that $x^3 \equiv 1 \pmod{31}$.

Since $3^{30} \equiv 1 \pmod{31}$, but no smaller power of 3 is 1 mod 31, the cube roots of 1 are 3^{10} , 3^{20} , and $3^{30} \equiv 1 \pmod{31}$. We found above that $3^{10} \equiv 25 \pmod{31}$. It follows that

$$3^{20} \equiv (3^{10})^2 \equiv (-6)^2 \equiv 36 \equiv 5 \pmod{31}.$$

Thus the solutions are $x \equiv 1, 5, 25 \pmod{31}$.

- (6) (a) Solve the system of congruences $x \equiv 3 \pmod{7}$, $x \equiv 4 \pmod{9}$.
 The first congruence implies that $x = 7k + 3$. Then the second congruence becomes $7k + 3 \equiv 4 \pmod{9}$, or

$$7k \equiv 1 \pmod{9}.$$

Thus $k \equiv \frac{1}{7} \pmod{9}$, which we compute as

$$k \equiv \frac{1}{7} \equiv \frac{1}{-2} \equiv \frac{10}{-2} \equiv -5 \equiv 4 \pmod{9}.$$

By the Chinese Remainder Theorem,

$$x \equiv 7 \cdot 4 + 3 \equiv \boxed{31 \pmod{63}}.$$

- (b) Solve the system of congruences $x \equiv 2 \pmod{9}$, $x \equiv 4 \pmod{10}$, $x \equiv 6 \pmod{11}$.
 The first congruence implies that $x = 9k + 2$. Then the second congruence becomes $9k + 2 \equiv 4 \pmod{10}$, or $-k \equiv 2 \pmod{10}$. Thus

$$k \equiv -2 \equiv 8 \pmod{10}.$$

We can therefore combine the first two congruences via the Chinese Remainder Theorem into the single congruence

$$x \equiv 9 \cdot 8 + 2 \equiv 74 \pmod{90}.$$

Now this implies that $x = 90\ell + 74$. Plugging this into the third congruence gives $90\ell + 74 \equiv 6 \pmod{11}$, or $2\ell \equiv 9 \pmod{11}$. Thus

$$\ell \equiv \frac{9}{2} \equiv \frac{-2}{2} \equiv -1 \equiv 10 \pmod{11},$$

and by the Chinese Remainder Theorem,

$$x \equiv 90 \cdot 10 + 74 \equiv \boxed{974 \pmod{990}}.$$

- (c) Find all of the square roots of 1 mod 105.

By the Chinese Remainder Theorem, $x^2 \equiv 1 \pmod{105}$ is equivalent to the system of congruences

$$x^2 \equiv 1 \pmod{3}; \quad x^2 \equiv 1 \pmod{5}; \quad x^2 \equiv 1 \pmod{7}.$$

Since each of 3, 5, and 7 is prime, each of these congruences has only the two solutions ± 1 . There are then 8 solutions to $x^2 \equiv 1 \pmod{105}$, corresponding to the 8 ways to choose ± 1 in each of the three congruences. We can find the solutions again using the Chinese Remainder Theorem:

$$\begin{array}{llll} x \equiv 1 \pmod{3}; & x \equiv 1 \pmod{5}; & x \equiv 1 \pmod{7} & \Leftrightarrow x \equiv 1 \pmod{105} \\ x \equiv 1 \pmod{3}; & x \equiv 1 \pmod{5}; & x \equiv -1 \pmod{7} & \Leftrightarrow x \equiv 76 \pmod{105} \\ x \equiv 1 \pmod{3}; & x \equiv -1 \pmod{5}; & x \equiv 1 \pmod{7} & \Leftrightarrow x \equiv 64 \pmod{105} \\ x \equiv 1 \pmod{3}; & x \equiv -1 \pmod{5}; & x \equiv -1 \pmod{7} & \Leftrightarrow x \equiv 34 \pmod{105} \\ x \equiv -1 \pmod{3}; & x \equiv 1 \pmod{5}; & x \equiv 1 \pmod{7} & \Leftrightarrow x \equiv 71 \pmod{105} \\ x \equiv -1 \pmod{3}; & x \equiv 1 \pmod{5}; & x \equiv -1 \pmod{7} & \Leftrightarrow x \equiv 41 \pmod{105} \\ x \equiv -1 \pmod{3}; & x \equiv -1 \pmod{5}; & x \equiv 1 \pmod{7} & \Leftrightarrow x \equiv 29 \pmod{105} \\ x \equiv -1 \pmod{3}; & x \equiv -1 \pmod{5}; & x \equiv -1 \pmod{7} & \Leftrightarrow x \equiv 104 \pmod{105} \end{array}$$

Thus the eight square roots of 1 mod 105 are $\boxed{1, 29, 34, 41, 64, 71, 76, \text{ and } 104 \pmod{105}}$.

(7) Let n be odd and composite. Show that there is an a with $1 \leq a < n$, $\gcd(a, n) = 1$, and

$$a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}.$$

First suppose that n is divisible by the square of a prime p , and let $n = p^k m$, where $\gcd(p, m) = 1$. Let g be a primitive root mod p^k , and let a be a solution with $1 \leq a < n$ to the system of congruences

$$x \equiv g \pmod{p^k}; \quad x \equiv 1 \pmod{m},$$

which exists by the Chinese Remainder Theorem. Then $\gcd(a, n) = 1$, since $\gcd(a, p^k) = 1$ and $\gcd(a, m) = 1$. Now the order of a mod p^k is $\phi(p^k) = p^k - p^{k-1}$, which is divisible by p since $k \geq 2$. On the other hand, $n - 1$ is certainly not divisible by p , since n is divisible by p . It follows that $a^{n-1} \not\equiv 1 \pmod{p^k}$. But if $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$, then upon squaring both sides,

$$a^{n-1} \equiv \left(\frac{a}{n}\right)^2 \equiv (\pm 1)^2 \equiv 1 \pmod{n}.$$

This contradiction shows that $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$, as desired.

Next suppose that n is squarefree. Let $n = pm$, where p is a prime. Let g be a primitive root mod p , and let a be a solution with $1 \leq a < n$ to the system of congruences

$$x \equiv g \pmod{p}; \quad x \equiv 1 \pmod{m},$$

which exists by the Chinese Remainder Theorem. Then $\gcd(a, n) = 1$. Now if $(p-1) \nmid (n-1)$, then $a^{n-1} \not\equiv 1 \pmod{p}$, and so $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right)$ as above. So we may assume that $(p-1) \mid (n-1)$, let's say $(n-1) = k(p-1)$. If k is even, then

$$a^{(n-1)/2} \equiv (a^{(p-1)/2})^k \equiv \left(\frac{a}{p}\right)^k \equiv (-1)^k \equiv 1 \pmod{p},$$

but

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) \left(\frac{a}{m}\right) = \left(\frac{g}{p}\right) \left(\frac{1}{m}\right) = -1.$$

Finally, suppose that n is squarefree, $(p-1) \mid (n-1)$ for all $p \mid n$, and $(n-1) = k(p-1)$ with k odd for each $p \mid n$. (Note that such numbers do actually exist; the smallest one is 8911.) Let $n = pqm$, where p and q are distinct odd primes, and let $n-1 = k(p-1)$, where k is odd. Let g and h be quadratic nonresidues mod p and q , respectively. Let a be a solution with $1 \leq a < n$ to the system of congruences

$$x \equiv g \pmod{p}; \quad x \equiv h \pmod{q}; \quad x \equiv 1 \pmod{m},$$

which exists by the Chinese Remainder Theorem. Then $\gcd(a, n) = 1$. Now

$$a^{(n-1)/2} \equiv (a^{(p-1)/2})^k \equiv \left(\frac{a}{p}\right)^k \equiv \left(\frac{g}{p}\right)^k \equiv (-1)^k \equiv -1 \pmod{p},$$

but

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) \left(\frac{a}{q}\right) \left(\frac{a}{m}\right) = \left(\frac{g}{p}\right) \left(\frac{h}{q}\right) \left(\frac{1}{m}\right) = (-1)(-1) = 1.$$

Remark. The structure of this proof is really to note that the result is immediate unless $a^{n-1} \equiv 1 \pmod{n}$ for all a with $\gcd(a, n) = 1$. Such n do exist (the smallest is 561), and are called *Carmichael numbers*. We can then deal with the Carmichael numbers by constructing an a for which the Jacobi symbol $\left(\frac{a}{n}\right)$ does not accurately predict whether a is a square mod n .

In fact, one can prove that $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$ for at least half of the values of a in the range $1 \leq a < n$. This observation leads to the *Solovay-Strassen primality test*, in which numbers a are chosen at random, and $\left(\frac{a}{n}\right)$ and $a^{(n-1)/2}$ are computed and compared. If they ever disagree, n is known to be composite; if they agree for a large number of random values of a , then a is prime with high probability.