

**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)  $2^{138} \pmod{213}$
  - (b)  $3^{173} \pmod{215}$
  - (c)  $5^{216} \pmod{217}$
- (2) Determine which of the following congruences are solvable:
- (a)  $x^2 \equiv 3 \pmod{17}$
  - (b)  $x^2 \equiv 3 \pmod{19}$
  - (c)  $x^2 \equiv 5 \pmod{19}$
  - (d)  $x^2 \equiv 3 \pmod{323}$
  - (e)  $x^3 \equiv 5 \pmod{19}$
  - (f)  $x^5 \equiv 5 \pmod{19}$
  - (g)  $x^9 \equiv 5 \pmod{19}$
- (3) Calculate the following Legendre symbols:
- (a)  $\left(\frac{22}{97}\right)$
  - (b)  $\left(\frac{35}{97}\right)$
  - (c)  $\left(\frac{-56}{97}\right)$
- (4) Solve the following congruences:
- (a)  $x^2 \equiv 5 \pmod{19}$
  - (b)  $x^5 \equiv 2 \pmod{19}$
  - (c)  $2^x \equiv 5 \pmod{19}$
- (5) (a) Find a primitive root mod 31.  
(b) Find all values of  $x$  such that  $x^3 \equiv 1 \pmod{31}$ .
- (6) (a) Solve the system of congruences  $x \equiv 3 \pmod{7}$ ,  $x \equiv 4 \pmod{9}$ .  
(b) Solve the system of congruences  $x \equiv 2 \pmod{9}$ ,  $x \equiv 4 \pmod{10}$ ,  $x \equiv 6 \pmod{11}$ .  
(c) Find all of the square roots of 1 mod 105.
- (7) Let  $n$  be odd and composite. Show that there is an  $a$  with  $1 \leq n < a$ ,  $\gcd(a, n) = 1$ , and

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