

Math 104B Winter 2003, Midterm 1: What's on the test?

5 Questions: 3 calculations, 2 proofs.

Here is a list of possible questions.

Define:

1. Order of a modulo p .
2. Primitive root.
3. Minimal universal exponent $\lambda(m)$.
4. The discrete logarithm of y to the base g modulo m .
5. Quadratic residue modulo m ; quadratic non-residue modulo m .
6. Legendre symbol $\left(\frac{a}{p}\right)$.

Prove:

1. If $a^k \equiv 1 \pmod{m}$ then $\text{ord}_m(a) | k$.
2. If $(a, m) = 1$ then $a^k \equiv a^j \pmod{m} \Leftrightarrow k \equiv j \pmod{\text{ord}_m(a)}$.
3. If $(a, m) = 1$ then $\text{ord}_m(a^k) = \text{ord}_m(a) / (k, \text{ord}_m(a))$.
4. There is no primitive root modulo 2^k if $k \geq 3$.
5. If $(m, n) = 1$ and $m > 2$, $n > 2$ then there is no primitive root modulo mn .
6. If $(a, m) = (b, m) = 1$, there exists c with $\text{ord}_m(c) = [\text{ord}_m(a), \text{ord}_m(b)]$.
7. The maximum possible order of elements modulo m is $\lambda(m)$.
8. If p is prime then there exists a primitive root modulo p .
9. If $(m, n) = 1$ and $(x, mn) = 1$ then $\text{ord}_{mn}(x) = [\text{ord}_m(x), \text{ord}_n(x)]$.
10. Euler's criterion.
11. Theorem 7.4.1.
12. If $m = a^2 + b^2$ and $n = x^2 + y^2$ then mn is also a sum of two squares.
13. If a prime $q = a^2 + b^2$ divides $n = x^2 + y^2$ then n/q is a sum of two squares.

Find: (for given values of a, b, c, m, r, p)

1. The order of a modulo m .
2. Whether there exists a primitive root modulo m .
3. One/all the primitive roots modulo m .
4. The number of elements of order d modulo m .
5. One/all elements of order d modulo m .
6. The value $\lambda(m)$.
7. The value of the Legendre symbol $\left(\frac{a}{m}\right)$.
8. One/all quadratic residues/non-residues modulo m ;
9. All the solutions to $x^{2^r} \equiv 1 \pmod{p}$.
10. The solutions to $x^2 \equiv a \pmod{m}$, or more generally $ax^2 + bx + c \equiv 0 \pmod{m}$.
11. The solution to an equation like $b^x \equiv c \pmod{m}$.
12. Whether m is a sum of two squares.
13. Numbers x and y so that $x^2 + y^2 = m$.