

## Math 104B Winter 2003, Final: What's on the test?

8 Questions: 5 calculations, 3 proofs.

Below is a list of possible questions. **You should be able to state all the definitions we have introduced during the course.**

**Prove:**

1. If  $a^k \equiv 1 \pmod{m}$  then  $\text{ord}_m(a) | k$ .
2. If  $(a, m) = 1$  then  $\text{ord}_m(a^k) = \text{ord}_m(a) / (k, \text{ord}_m(a))$ .
3. If  $p$  is prime then there exists a primitive root modulo  $p$ .
4. If the prime  $p$  divides a sum of two relatively prime squares then  $p \equiv 1 \pmod{4}$ .
5. Gauss's Lemma.
6. If  $n(p)$  is the number of elements of  $S = \{a, 2a, \dots, \frac{p-1}{2}a\}$  which are negative when expressed in the absolute least residue system modulo  $p$ , then

$$n(p) = \sum_{j=1, j \text{ odd}}^{a-1} \left( \left\lfloor \frac{(j+1)p}{2a} \right\rfloor - \left\lfloor \frac{jp}{2a} \right\rfloor \right).$$

7. If  $p \equiv \pm q \pmod{4a}$  then  $n(p) \equiv n(q) \pmod{2}$ .
8. If  $[a_0, a_1, \dots]$  is an infinite continued fraction with  $a_j \geq 1$  for  $j \geq 1$  then  $C_{2k}$  is an increasing sequence,  $C_{2k+1}$  is a decreasing sequence, and  $C_k$  tends to a limit as  $k \rightarrow \infty$ .
9. The continued fraction expansion of a quadratic irrational is eventually periodic.
10. If a quadratic irrational  $x$  satisfies  $x > 1$  and  $-1 < \bar{x} < 0$ , then its continued fraction expansion is purely periodic.
11. (Theorem of Lagrange) If  $p$  is a prime with  $p \equiv 1 \pmod{4}$ , then  $x^2 - py^2 = -1$  has a solution.
12. If  $x, y, z$  solves  $x^4 + y^4 = z^4$ , then  $xyz = 0$ .

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

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  $b^x \equiv c \pmod{m}$ .

(continued on the next page)

12. Whether  $m$  is a sum of two squares.
13. Numbers  $x$  and  $y$  so that  $x^2 + y^2 = m$ .
14. The primes which divide  $x^2 - a$  for some  $x$ .
15. The value of the Jacobi symbol  $\left(\frac{a}{m}\right)$ .
16. The convergents of the continued fraction expansion of  $p/q$ .
17. The continued fraction expansion of  $a + b\sqrt{m}$ .
18. Numbers  $x$  and  $y$  such that  $x^2 + y^2 = p$ , where  $p/q = [a_0, \dots, a_j, a_j, \dots, a_0]$ .
19. The first few terms of the continued fraction expansion of  $a^{1/p}$ .
20. The number  $[b_0, \dots, b_m, \overline{a_1, \dots, a_n}]$  (the  $a_i$ s and  $b_j$ s are given).
21. whether  $p/q$  is a best approximation to  $x$ .
22. The first few solutions  $x, y$  of  $x^2 - dy^2 = 1$
23. The first few solutions  $x, y$  of  $x^2 - dy^2 = -1$
24. Whether there is a solution to  $x^2 - dy^2 = m$