Math 3240/Roby **Review & Practice Final** December 2012

Answer all the questions below before coming to the review session on Sunday 9 December, 3-5 PM in MSB 215. The final exam is Tuesday 11 December, 1–3 PM in MSB 215.

SHOW ALL YOUR WORK! Make sure you give reasons to support your answers. If you have any questions, do not hesitate to ask! The final examination is cumulative, covering everything from the beginning of the course, with somewhat heavier emphasis on later material. You may use one $4'' \times 6''$ index card (both sides) to include any notes you think you might like to have.

Definitions

1. Give a definition of a unit and a prime which works at the same time in all the following examples: $\mathbf{Z}$, $\mathbf{Z}[\sqrt{d}]$, $\mathbf{Q}[x]$, $\mathbf{R}[x]$, $\mathbf{F}_p[x]$.
2. What is the order of a unit a mod m?
3. What are the Legendre symbol $(\frac{a}{p})$ and the Jacobi symbol $(\frac{a}{n})$? (Defining these includes indicating what the meaning of the parameters in the symbols is.)
4. What is a Fermat witness? An Euler witness?

Numerical Examples

5. What are the possible orders of units mod 19? Find the order of 5 mod 19.
6. Give a formula for $\varphi(m)$ in terms of the prime factorization of m and compute $\varphi(108)$.
7. Find the decoding function corresponding to the RSA encoding function $E(x) = x^5$ mod 65.
8. Factor $1 + 5i$, $3 + 4i$, and $4 + 7i$ into primes in $\mathbf{Z}[i]$. (Hint: Factor their norms in $\mathbf{Z}$ first.)
9. Compute the following Legendre symbols: $(\frac{10}{31})$ and $(\frac{-30}{103})$.
10. Does $x^2 + x + 11 \equiv 0 \bmod 37$ have any solutions? What about $x^2 + x + 11 \equiv 0 \bmod 203$?

Squares

14. If $(m, n) = 1$ in $\mathbf{Z}$, show $a \equiv \square \bmod mn \iff a \equiv \square \bmod m$ and $a \equiv \square \bmod n$.
15. For odd prime p, show there are $\frac{p-1}{2}$ nonzero squares in $\mathbf{Z}/p$ and $\frac{p-1}{2}$ nonsquares in $\mathbf{Z}/p$.
16. Prove Euler's congruence $a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \bmod p$ for odd prime p and $a \not\equiv 0 \bmod p$ and use it to derive a formula for $(\frac{-1}{p})$. Is there anything logically wrong with deriving Fermat's little theorem from Euler's congruence by squaring both sides of Euler's congruence?
17. Use Euler's congruence to show the Legendre symbol is totally multiplicative in the numerator: $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ for all integers a and b.
18. State (using complete sentences with correct quantifiers) the quadratic reciprocity law: the main law and the two supplementary laws.

Miscellaneous

19. List some practical applications (i.e., uses which your friends regularly come into contact with, whether they realize it or not) of modular arithmetic.

20. State and explain divisibility rules for each integer 2–11 (except 7). Write careful proofs for 4, 8 and 11.

21. If $d|m$, show $d|(a+m) \iff d|a$.

22. If a mod m has order n, show for $k \geq 1$ that $a^k \equiv 1 \bmod m$ if and only if $n|k$.

23. Show a composite number n has a nontrivial factor that is $\leq \sqrt{n}$.

24. Show a sum of two squares in $\mathbf{Z}$ is not 3 mod 4. Are there any congruence classes that cannot be a sum of two cubes mod 7? Mod 9?

25. Show the equation $x^2 - 11y^2 = 51$ has no integral solution. (Hint: Use modular arithmetic with a well-chosen modulus.)

26. Assuming that the norm on $\mathbf{Z}[\sqrt{d}]$ is multiplicative, show an element of $\mathbf{Z}[\sqrt{d}]$ whose norm is prime in $\mathbf{Z}$ is prime in $\mathbf{Z}[\sqrt{d}]$. Then give an example of a prime element of $\mathbf{Z}[\sqrt{10}]$.

27. Go over all the problems on the quizzes, practice midterm, midterm, and homework, with special attention to any "learning opportunities" you may have encountered.