Homework Assignment 3
Due Wednesday October 16

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2002**

Instructions: *Please work with others,* and acknowledge who you work with in your write up. Some of these problems will require a computer; others look like a computer might be helpful, but in fact it isn't. If you use a computer, please describe how you use the computer (you are *not* required to use MAGMA).

1. (2 points each) Find all solutions to the following quadratic equations using the quadratic formula over $\mathbb{Z}/p$ and the algorithms from class. Describe how you use the algorithm, but use a computer for the tedious computations.

   (a) $19x^2 + 1783x + 29485 = 0$ over $\mathbb{Z}/29527$.

   (b) $x^2 + 2^{87} = 0$ over $\mathbb{Z}/(2^{89} - 1)$.

   (c) $x^2 + 2^{47} = 0$ over $\mathbb{Z}/(2^{53} + 5)$.

2. (6 points) During my lecture on Friday, I suggested that a web page assumed that in the square root algorithm I gave, either u or v must always be 0. Here $u, v \in \mathbb{Z}/p$ were defined by an equation of the form $u + vx = (1 + zx)^{\frac{p-1}{2}}$ (see Section 6.5 of the notes). Either prove this assertion or give a counterexample.

3. (8 points) Research the following: What is the current status of the RSA patent? Could you write a commercial program that implements the RSA cryptosystem without having to pay anyone royalties? What about a free program? Same questions, but for the Diffie-Hellman key exchange.

4. For any positive integer n, let $\sigma(n)$ be the sum of the divisors of n; for example, $\sigma(6) = 1 + 2 + 3 + 6 = 12$ and $\sigma(10) = 1 + 2 + 5 + 10 = 18$.

   (a) (10 points) Suppose that $n = pqr$ with p, q, and r primes. Devise an "efficient" algorithm that given n, $\varphi(n)$ and $\sigma(n)$, computes the factorization of n. For example, if $n = 105$, then $p = 3$, $q = 5$, and $r = 7$, so the input to the algorithm would be
   $$n = 105, \qquad \varphi(n) = 48, \qquad \text{and} \quad \sigma(n) = 192,$$
   and the output would be 3, 5, 7.

   (b) (3 points) Use your algorithm to factor $n = 60071026003$ given that $\varphi(n) = 60024000000$ and $\sigma(n) = 60118076016$.

5. (6 points) Let p be a prime and let ζ be a primitive pth root of unity. Prove that every $\mathbb{Z}$-linear combination of powers of ζ can be written uniquely as a $\mathbb{Z}$-linear combination of elements of $B = \{1, \zeta, \ldots, \zeta^{p-2}\}$. [Hint: $\zeta^p - 1 = 0$, so $\zeta^{p-1} + \cdots + \zeta + 1 = 0$, so $\zeta^{p-1} = -(\zeta^{p-2} + \cdots + \zeta + 1)$. Next prove somehow that the polynomial $x^{p-1} + \cdots + x + 1$ does not factor over $\mathbb{Q}$. I might not have told you enough in the course to do this, so be resourceful.]