T-79.503 Foundations of Cryptology
Homework 10
November 25, 2004

1. (a) Evaluate the following Jacobi symbol using the four properties presented in Section 5.4. You should not do any factoring other than dividing out powers of 2.

$$\left(\frac{2777}{4453}\right).$$

   (b) Show that $4453 = 61 \cdot 73$ is an Euler pseudoprime to the base 2777.

2. (a) Find all square roots of 1 modulo 4453.

   (b) 2777 is a square root of 3586 modulo 4453. Find all square roots of 3586 modulo 4453.

3. The integers 26945 and 459312 are square roots of the integer 80833 modulo 540143. Based on this information find some nontrivial integer divisors of 540143.

4. (Stinson 5.24. This result can be used to prove Theorem 5.12) Suppose throughout this question that p is an odd prime and $\gcd(a, p) = 1$.

   a) Suppose that $i \geq 2$ and $b^2 \equiv a \pmod{p^{i-1}}$. Prove that there is a unique $x \in \mathbb{Z}_p^i$, such that $x^2 \equiv a \pmod{p^i}$ and $x \equiv b \pmod{p^{i-1}}$. Describe how this x can be computed efficiently.

   b) Illustrate your method in the following situation: starting with the congruence $6^2 \equiv 17 \pmod{19}$, find square roots of 17 modulo 19^2 and modulo 19^3.

5. The integer $n = 89855713$ is known to be a product of two primes. Further, it is given that $\phi(n) = 89836740$. Determine the factors of n.

6. Attempt to find factors of 121939 using the $p - 1$ method with $B = 6$.