Test 2 for Spring/2004

Due by May 7, 2004

***1.** Show that $x^2 \equiv y^2$ $(mod\ n)$ and $x \not\equiv \pm y$ $(mod\ n)$, then $gcd(x+y, n)$ is a nontrivial factor of n.

2. Prove that $2^n - 1$ is prime implies that n is prime.

3. Prove or disprove that $2^{2^n} - 1$ is a prime number if n is prime.

4. Test if the following integers are prime or not. If it is not prime, factor it.

(a) 65537

(b) 632887

5. Let $n = pq$ be the product of two primes.

(a) Suppose that $m \equiv 0$ $(mod\ \phi(n))$. Show that if $gcd(a, n) = 1$, then $a^m \equiv 1$ $(mod\ p)$ and $a^m \equiv 1$ $(mod\ q)$.

(b) Suppose that $m \equiv 0$ $(mod\ \phi(n))$ and let a be arbitrary (possibly $gcd(a, n) \neq 1$). Show that $a^{m+1} \equiv a$ $(mod\ p)$ and $a^{m+1} \equiv a$ $(mod\ q)$.

(c) Let e and d be encryption and decryption exponents for RSA with *modulus* n. Show that $a^{ed} \equiv a$ $(mod\ n)$ for all a. *This problem shows that we do not need to assume that* $gcd(a, n) = 1$ *in order to use RSA.*

(d) If p and q are large, why is it likely that $gcd(a, n) = 1$ for a randomly chosen a?

6. Solve $3^x \equiv 24$ $(mod\ 31)$

7. Let $p = 3989$ be a prime number.

(a) Show that $L_2(3925) = 2000$ and $L_2(1046) = 3000$.

(b) Evaluate $L_2(3925 \cdot 1046)$.

***8.** Use the Pohlig-Hellman algorithm to solve $11^x \equiv 2$ $(mod\ 1201)$

(Hint) $1201 - 1 \;=\; 1200 \;=\; 2^4 \cdot 3 \cdot 5^2$