
(a) Let $p$ be an odd prime and $b$ an integer not divisible by $p$. Prove that either $b$ has two square roots modulo $p$ or else it has no square roots modulo $p$. In other words show that the equation

$$x^2 \equiv b \pmod{p}$$

has either 0 or two solutions. (What happens when $p = 2$?)

(b) Find the square roots of $b$ modulo $p$ for the following values.

(i) $(p, b) = (7, 2)$.

(ii) $(p, b) = (11, 7)$.

(iii) $(p, b) = (11, 5)$.

(iv) $(p, b) = (37, 3)$.

(c) How many square roots does 29 have modulo 35?

(d) Let $g$ be a primitive root for $(\mathbb{Z}/p\mathbb{Z})^*$. Thus every nonzero element $a \in (\mathbb{Z}/p\mathbb{Z})^*$ is equal to $g^k$ for some $k$. Prove that $a$ has a square root if and only if $k$ is even.

Problem 2. A prime of the form $2^n - 1$ is called a Mersenne prime.

(a) Factor each of the numbers $2^n - 1$ for $n = 2, 3, \ldots, 10$. Which ones are Mersenne primes?

(b) Find the first seven Mersenne primes.

(c) If $n$ is even and $n > 2$, prove that $2^n - 1$ is not prime.

(d) If $3|n$ and $n > 3$, prove that $2^n - 1$ is not prime.

(e) More generally, prove that if $n$ is a composite number then $2^n - 1$ is not prime. Thus all Mersenne primes are of the form $2^p - 1$ where $p$ is prime.

(f) What is the largest known Mersenne prime? Are there any larger primes known? You can find out at the “Great Mersenne Prime Search” website: www.mersenne.org/prime.htm.

Problem 3. Use Pollard’s $p - 1$ method to factor each of the following numbers. Show your work, and be sure to indicate which factor has the property that $p - 1$ is a product of small primes.

(a) $n = 1739$.

(b) $n = 220459$.

(c) $n = 48356747$.

Problem 4. For each part, use the data provided to find values of $a$ and $b$ satisfying $a^2 \equiv b^2 \pmod{N}$, and then compute $\gcd(N, a - b)$ in order to find a nontrivial factor of $N$.

(a) $N = 61063$

$$
1882^2 \equiv 270 \pmod{N} \quad \text{and} \quad 270 = 2 \cdot 3^3 \cdot 5
$$

$$
1898^2 \equiv 60750 \pmod{N} \quad \text{and} \quad 60750 = 2 \cdot 3^5 \cdot 5^3
$$

(b) $N = 52907$

$$
399^2 \equiv 480 \pmod{N} \quad \text{and} \quad 480 = 2^5 \cdot 3 \cdot 5
$$

$$
763^2 \equiv 192 \pmod{N} \quad \text{and} \quad 192 = 2^6 \cdot 3
$$

$$
773^2 \equiv 15552 \pmod{N} \quad \text{and} \quad 15552 = 2^6 \cdot 3^5
$$

$$
976^2 \equiv 250 \pmod{N} \quad \text{and} \quad 250 = 2 \cdot 5^3
$$
 Problem 5. Here is an example of a public key cryptosystem that was actually proposed at a cryptography conference. It is supposed to be faster and more efficient than RSA.

Alice chooses two large primes $p$ and $q$ and she publishes $N = pq$. It is assumed that $N$ is hard to factor. Alice also chooses three random numbers $g$, $r_1$ and $r_2$ modulo $N$ and computes

$$g_1 \equiv g^{r_1(p-1)} \pmod{N} \quad \text{and} \quad g_2 \equiv g^{r_2(q-1)} \pmod{N}.$$  

Her public key is the triple $(N, g_1, g_2)$ and her private key is the pair of primes $(p, q)$.

Now Bob wants to send the message $m$ to Alice, where $m$ is a number modulo $N$. He chooses two random integers $s_1$ and $s_2$ modulo $N$ and computes

$$c_1 \equiv mg_1^{s_1} \pmod{N} \quad \text{and} \quad c_2 \equiv mg_2^{s_2} \pmod{N}.$$  

Bob sends the ciphertext $(c_1, c_2)$ to Alice.

Decryption is extremely fast and easy. Alice uses the Chinese remainder theorem to solve the pair of congruences

$$x \equiv c_1 \pmod{p} \quad \text{and} \quad x \equiv c_2 \pmod{q}.$$  

(a) Prove that Alice’s solution $x$ is equal to Bob’s plaintext $m$.

(b) Explain why this cryptosystem is not secure. (Hint: making numbers such as $g_1$ or $g_2$ public is a bad idea — why?)