1 Modular Practice

Solve the following modular arithmetic equations for x and y.

(a) $9x + 5 \equiv 7 \pmod{11}$.

(b) Show that $3x + 15 \equiv 4 \pmod{21}$ does not have a solution.

(c) The system of simultaneous equations $3x + 2y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$.

(d) $13^{2019} \equiv x \pmod{12}$.

(e) $7^{67} \equiv x \pmod{11}$.

2 Fibonacci GCD

The Fibonacci sequence is given by $F_n = F_{n-1} + F_{n-2}$, where $F_0 = 0$ and $F_1 = 1$. Prove that, for all $n \geq 0$, $\gcd(F_n, F_{n-1}) = 1$.

3 RSA Warm-Up

Consider an RSA scheme with modulus $N = pq$, where p and q are distinct prime numbers larger than 3.

(a) What is wrong with using the exponent $e = 2$ in an RSA public key?

(b) Recall that e must be relatively prime to $p-1$ and $q-1$. Find a condition on p and q such that $e = 3$ is a valid exponent.

(c) Now suppose that $p = 5$, $q = 17$, and $e = 3$. What is the public key?

(d) What is the private key?

(e) Alice wants to send a message $x = 10$ to Bob. What is the encrypted message $E(x)$ she sends using the public key?

(f) Suppose Bob receives the message $y = 24$ from Alice. What equation would he use to decrypt the message? and what is the decrypted message?

4 Breaking RSA

Eve is not convinced she needs to factor $N = pq$ in order to break RSA. She argues: "All I need to know is $(p-1)(q-1)$... then I can find d as the inverse of e mod $(p-1)(q-1)$. This should be easier than factoring N." Prove Eve wrong, by showing that if she knows $(p-1)(q-1)$, she can easily factor N (thus showing finding $(p-1)(q-1)$ is at least as hard as factoring N).