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

Solution:

(a) Subtract 5 from both sides to get:

$$9x \equiv 2 \pmod{11}.$$

Now since $\gcd(9,11)=1$, 9 has a (unique) inverse mod 11, and since $9\times 5 = 45 \equiv 1 \pmod{11}$ the inverse is 5. So multiply both sides by $9^{-1} \equiv 5 \pmod{11}$ to get:

$$x \equiv 10 \pmod{11}.$$

(b) Subtract 15 from both sides to get:

$$3x \equiv 10 \pmod{21}.$$

Now note that this implies $3x \equiv 1 \pmod 3$, since 3 divides 21, and the latter equation has no solution, so the former cannot either.

We are using the fact that if $d \mid m$, then $x \equiv y \pmod m$ implies $x \equiv y \pmod d$ (but not necessarily the other way around). To see this, if $x \equiv y \pmod m$, then $m \mid x-y$ (by definition) and so $d \mid x-y$, and hence $x \equiv y \pmod d$.

(c) First, subtract the first equation from double the second equation to get:

$$2(2x+y)-(3x+2y) \equiv x \equiv 1 \pmod 7.$$

Now plug into the second equation to get:

$$2+y \equiv 4 \pmod 7,$$

so the system has the solution $x \equiv 1 \pmod 7$, $y \equiv 2 \pmod 7$.

(d) 13 is always 1 mod 12, so 13 to any power mod 12 is 1.

$$13^{2019} \equiv 1^{2019} \equiv 1 \pmod{11}.$$

(e) We can use repeated squaring for this question.

$7^2 \equiv 5 \pmod{11}$
$7^4 \equiv (7^2)^2 \equiv 5^2 \equiv 3 \pmod{11}$
$7^8 \equiv (7^4)^2 \equiv 3^2 \equiv 9 \pmod{11}$
$7^{16} \equiv (7^8)^2 \equiv 9^2 \equiv 4 \pmod{11}$
$7^{32} \equiv (7^{16})^2 \equiv 4^2 \equiv 5 \pmod{11}$
$7^{64} \equiv (7^{32})^2 \equiv 5^2 \equiv 3 \pmod{11}$
$7^{67} \equiv 7^{64} \times 7^2 \times 7^1 \equiv 3 \times 5 \times 7 \pmod{11}$
$7^{67} \equiv 3 \times 35 \equiv 3 \times 2 \equiv 6 \pmod{11}$.

A way to avoid repeated squaring for so many times is to use Fermat's Little theorem to simplify the exponent. We can rewrite the exponent as $67 = (11-1) \times 6 + 7$, and this will give us:

$$\begin{aligned} 7^{(10\times 6+7)} &\equiv (7^{10})^6 \times 7^7 \pmod{11} \\ &\equiv 1^6 \times 7^7 \pmod{11} \\ &\equiv 7^7 \pmod{11}. \end{aligned}$$

From this step, we can easily simplify it into:

$$\begin{aligned} (7^2)^3 \times 7 \pmod{11} &\equiv 5^3 \times 7 \pmod{11} \\ &\equiv 4 \times 7 \pmod{11} \\ &\equiv 28 \pmod{11} \\ &\equiv 6 \pmod{11}. \end{aligned}$$

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 $n \geq 0$, $\gcd(F_n, F_{n-1}) = 1$.

Solution:

Proceed by induction.

Base Case: We have $\gcd(F_1, F_0) = \gcd(1, 0) = 1$, which is true.

Inductive Hypothesis: Assume we have $\gcd(F_k, F_{k-1}) = 1$ for some $k \geq 1$.

Inductive Step: Now we need to show that $\gcd(F_{k+1}, F_k) = 1$ as well.

We can show that:

$$\gcd(F_{k+1}, F_k) = \gcd(F_k + F_{k-1}, F_k) = \gcd(F_k, F_{k-1}) = 1.$$

Note that the second expression comes from the definition of Fibonacci numbers. The last expression comes from Euclid's GCD algorithm, in which $\gcd(x, y) = \gcd(y, x \bmod y)$, since

$$F_k + F_{k-1} \equiv F_{k-1} \pmod{F_k}.$$

Therefore the statement is also true for $n = k+1$.

By the rule of induction, we can conclude that $\gcd(F_n, F_{n-1}) = 1$ for all $n \geq 1$, where $F_0 = 0$ and $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$.

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?

Solution:

(a) To find the private key d from the public key (N, e), we need $\gcd(e, (p-1)(q-1)) = 1$. However, $(p-1)(q-1)$ is necessarily even since p, q are distinct odd primes, so if $e = 2$, $\gcd(e, (p-1)(q-1)) = 2$, and a private key does not exist. (Note that this shows that e should more generally never be even.)

(b) Both p and q must be of the form $3k+2$. $p = 3k+1$ is a problem since then $p-1$ has a factor of 3 in it. $p = 3k$ is a problem because then p is not prime.

(c) $N = p \cdot q = 85$ and $e = 3$ are displayed publicly. Note that in practice, p and q should be much larger (512-bit) numbers. We are only choosing small numbers here to allow manual computation.

(d) We must have $ed = 3d \equiv 1 \pmod{64}$, so $d = 43$. Reminder: we would do this by using extended gcd with $x = 64$ and $y = 3$. We get $\gcd(x,y) = 1 = ax + by$, and $a = 1$, $b = -21$.

(e) We have $E(x) = x^3 \pmod{85}$, where $E(x)$ is the encryption function. $10^3 \equiv 65 \pmod{85}$, so $E(x) = 65$.

(f) We have $D(y) = y^{43} \pmod{85}$, where $D(y)$ is the decryption function, the inverse of $E(x)$.

$$\begin{aligned}
24^{43} &\equiv 8^{43} \times 3^{43} \pmod{85} \\
&\equiv (2^3)^{43} \times 3^{43} \pmod{85} \\
&\equiv 2^{129} \times 3^{43} \pmod{85} \\
&\equiv 2^{129} \times 3^{4\times 10+3} \pmod{85} \\
&\equiv 2^{129} \times 81^{10} \times 3^3 \pmod{85} \\
&\equiv 2^{129} \times (-4)^{10} \times 3^3 \pmod{85} \\
&\equiv 2^{129} \times 2^{20} \times 3^3 \pmod{85} \\
&\equiv 2^{149} \times 3^3 \pmod{85} \\
&\equiv 2^{8\times 18+5} \times 3^3 \pmod{85} \\
&\equiv 256^{18} \times 2^5 \times 3^3 \pmod{85}.
\end{aligned}$$

We have $256 - 3 * 85 = 1$. So

$$\begin{aligned}
24^{43} &\equiv 1^{18} \times 2^5 \times 3^3 \pmod{85} \\
&\equiv 32 \times 3 \times 3^2 \pmod{85} \\
&\equiv 96 \times 3^2 \pmod{85} \\
&\equiv 11 \times 9 \pmod{85} \\
&\equiv 99 \equiv 14 \pmod{85},
\end{aligned}$$

so $D(y) = 14$.

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).

Solution:

Let $a = (p-1)(q-1)$. If Eve knows $a = (p-1)(q-1) = pq - (p+q) + 1$, then she knows

$$N - q - p + 1 = a,$$

$$pq = N.$$

We can write q as $N - p - a + 1$ and substitute into the second equation:

$$p(N - p - a + 1) = N.$$

Then we get the following quadratic function for p:

$$p^2 + (a - N - 1)p + N = 0.$$

We can easily solve this equations and obtain p and q. This is equivalent to factoring N.