1

By definition $6x^2 + 5x + 1 \equiv_p 0$ infers that

$$p | 6x^2 + 5x + 1$$

which validates the following for some $k \in \mathbb{Z}$

$$pk = 6x^2 + 5x + 1$$

$$6x^2 + 5x + 1 - pk = 0$$

Now, assume I can factor the above equation into

$$(3x - w)(2x + w) = 0$$

For some $w \in \mathbb{Z}$ which satisfies both

$$3w - 2w = 5x$$

$$w^2 = 1 - pk$$

Then

That

Now, if I can find a $x \in \mathbb{Z}$ that satisfies $3w - 2w = 5x$ and $w^2 = 1 - pk$ and where k

2

$$\begin{aligned}
n_1 = 2, \quad c_1 = 1, \quad m_1 = 105, \quad 105d_1 \equiv_2 1, \quad d_1 = 1 \\
n_2 = 3, \quad c_2 = 2, \quad m_2 = 70, \quad 70d_2 \equiv_3 1, \quad d_2 = 1 \\
n_3 = 5, \quad c_3 = 0, \quad m_3 = 42, \quad 42d_3 \equiv_5 1, \quad d_3 = 3 \\
n_4 = 7, \quad c_4 = 3, \quad m_4 = 30, \quad 30d_4 \equiv_7 1, \quad d_4 = 4
\end{aligned}$$

Hence

$$x \equiv_{210} 1 \cdot 105 \cdot 1 + 2 \cdot 70 \cdot 1 + 0 \cdot 42 \cdot 3 + 3 \cdot 30 \cdot 4 \equiv_{210} 535 \equiv_{210} 115$$

$x \equiv_{210}$ **115**

3

$U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ The order and generated group of each unit is

$$\begin{aligned}
|1| = 1, \quad \langle 1 \rangle = \{1\} \\
|2| = 4, \quad \langle 2 \rangle = \{2, 4, 8, 2\} \\
|4| = 2, \quad \langle 4 \rangle = \{4, 1\} \\
|7| = 4, \quad \langle 7 \rangle = \{7, 4, 13, 1\} \\
|8| = 4, \quad \langle 8 \rangle = \{8, 4, 2, 1\} \\
|11| = 2, \quad \langle 11 \rangle = \{11, 1\} \\
|13| = 4, \quad \langle 13 \rangle = \{13, 4, 7, 1\} \\
|14| = 2, \quad \langle 14 \rangle = \{14, 1\}
\end{aligned}$$

No unit modulo 15 is able to generate the entire U_{15} group. Therefore U_{15} is not cyclic.

4

Since $n = 433$ is prime, $\phi(n) = N = 432 = 2^4 \cdot 3^3$.

$$N_1 = \frac{N}{2^4} = 27 \quad N_2 = \frac{N}{3^4} = 16$$

Now I will compute g_1, g_2, h_1, h_2

$$\begin{aligned} g_1 &\equiv_n 7^{27} \equiv_n 265 \\ g_2 &\equiv_n 7^{16} \equiv_n 374 \\ h_1 &\equiv_n 166^{27} \equiv_n 250 \\ h_2 &\equiv_n 166^{16} \equiv_n 335 \end{aligned}$$

Iterating over k until $g_i^k \equiv_n h_i$ is found
For g_1

$$\begin{aligned} 265^2 &\equiv_n 153 \\ 265^3 &\equiv_n 198 \\ &... \\ 265^{15} &\equiv_n 250 \end{aligned}$$

For g_2

$$\begin{aligned} 374^2 &\equiv_n 17 \\ 374^3 &\equiv_n 296 \\ &... \\ 374^{20} &\equiv_n 335 \end{aligned}$$

$$\begin{aligned} g_1^{15} &\equiv_n 265^{15} \equiv_n 250 \equiv_n h_1 &\Rightarrow k_1 = 15 \\ g_2^{20} &\equiv_n 374^{20} \equiv_n 335 \equiv_n h_2 &\Rightarrow k_2 = 20 \end{aligned}$$

Using this result I will calculate x using the Chinese Remainder theorem.

$$\begin{cases} x \equiv_{16} 15 \\ x \equiv_{27} 20 \end{cases}$$

$$\begin{aligned} x &= 15 + 16y \\ 15 + 16y &\equiv_{27} 20 \Rightarrow \\ &16y \equiv_{27} 5 \\ &y \equiv_{27} 5 \cdot 22 \\ &y \equiv_{27} 2 \\ x &= 15 + 32 + 432k \end{aligned}$$

One such solution is $x = \mathbf{47}$

5

Both g^a and g^b can be rewritten as

$$(g^m)^{a'}$$
$$(g^m)^{b'}$$

Where m is the order of g modulo n and $a' = \frac{a}{m}$, $b' = \frac{b}{m}$.
I know the values a' and b' exist because of this proof by contradiction.
Assume there is an x such that $g^x \equiv_n 1$ but $m \not| x$ where $m = |g|$. I then split x into components as follows. $x = a_0 m + a_1$ where $1 \leq a_1 < m$. Then

$$\begin{aligned} g^{a_0 m + a_1} \equiv_n 1 & \\ &= g^{a_0 m} \cdot g^{a_1} \equiv_n 1 \\ &= (g^m)^{a_0} \cdot g^{a_1} \equiv_n 1 \\ &= 1^{a_0} \cdot g^{a_1} \equiv_n 1 \\ &= g^{a_1} \equiv_n 1 \end{aligned}$$

With $1 \leq a_1 < m$ this is a contradiction, because if such a_1 were to exist it would itself be the order.
Now that I know such an $a', b' \in \mathbb{Z}$ and further that they share the divisor m, then let $d = gcd(a, b)$. $m|d$, so let $d' = \frac{d}{m}$

6

By expanding the defintion of c_1 and c_2 I get

$$\begin{cases} x \equiv_p m g_1^{s_1} \\ x \equiv_q m g_2^{s_2} \end{cases}$$

And then expanding g_1 and g_2 you get

$$\begin{cases} x \equiv_p m(g^{r_1(p-1)})^{s_1} \\ x \equiv_q m(g^{r_2(q-1)})^{s_2} \end{cases}$$

Then using proporties of exponentials

$$\begin{cases} x \equiv_p m(g^{s_1 r_1})^{(p-1)} \\ x \equiv_q m(g^{s_2 r_2})^{(q-1)} \end{cases}$$

Fermat's little theorem lets us cancel the $g^{\cdots}$ term

$$\begin{cases} x \equiv_p m \\ x \equiv_q m \end{cases}$$

Because p and q are pairwise prime the solution to this Chinese Remainder will be m

7

7.1

$$1794677960^{(32411-1)/2} \equiv_{32411} -1$$
$$525734818^{(32411-1)/2} \equiv_{32411} 1$$
$$420526487^{(32411-1)/2} \equiv_{32411} -1$$

Hence Alice's message is $1, 0, 1$

7.2

$N = 3149 = 47 \cdot 67$

$$2322^{(47-1)/2} \equiv_{47} -1$$
$$719^{(47-1)/2} \equiv_{47} 1$$
$$202^{(47-1)/2} \equiv_{47} 1$$

Hence Alice's message is $1, 0, 0$

7.3

$$(568980706 \cdot 705130839^2)\%781044643 = \mathbf{517254876}$$
$$(568980706 \cdot 631364468^2)\%781044643 = \mathbf{4308279}$$
$$(631364468^2)\%781044643 = \mathbf{111914931}$$

8

Using the problem definition I will define d, a', b'

$$d = gcd(a, b)$$
$$a' = \frac{a}{d}$$
$$b' = \frac{b}{d}$$

Consequently

$$gcd(a', b') = 1$$
$$(g^d)^{a'} \equiv_n (g^d)^{b'}$$

Using Lagranges Theorem, I know the only valid value for $g^d \equiv_n 1$

9

because $n = 433$ is prime $\phi(n) = n - 1 = 432 = 2^4 \cdot 3^3$. i will choose $n_1 = 2^4 = 16$, and $n_2 = 3^3 = 27$. next i will compute $g_1, g2, h_1, h_2$

$$g_1 = 7^{27} \equiv_n$$

10

10.1

show that n is a carmichael number
$n = 1729 = 7 \cdot 13 \cdot 19$ and hence it is composite. pick any a coprime with n. by fermats little theorem

$$a^6 \equiv_7 1$$
$$a^{12} \equiv_{13} 1$$
$$a^{18} \equiv_{19} 1$$

$n - 1 = 1728 = 2^6 \cdot 3^3$ so it is easy to see

$$1728/6 = 288 \to a^{1278} \equiv_7 (a^6)^{288} \equiv_7 1$$
$$1728/12 = 144 \to a^{1278} \equiv_{13} (a^{12})^{144} \equiv_{13} 1$$
$$1728/18 = 96 \to a^{1278} \equiv_{19} (a^{18})^{96} \equiv_{19} 1$$

hence, $a^{n-1} \equiv_n 1$ and n is carmichael

10.2

$n - 1 = 2^6 \cdot 27$ so using 3 as a base

$$3^{27} \equiv_{1728} 664$$
$$3^{2 \cdot 27} \equiv_{1729} 1$$

returns **not prime**
since 3 shows the compositeness of 1728 it is a miller-rabin witness.

11

using the given equiation

$$(763 \cdot 773)^2 \equiv_n (2^6 \cdot 3^3)^2$$

hence

$$a = 763 \cdot 773 = 589799$$
$$b = 2^6 \cdot 3^3 = 1728$$

so $gcd(52907, a - b) =$ **277** is a non-trivial factor of 52907

11.1

i only have to check values $\phi(n)/p_i$ where p_i is the i^{th} prime.

$$\phi(113) = 112 = 2^4 \cdot 7$$

avoiding redundent values, i will only check 56 and 16 for $g = 2$

$$2^{16} \equiv_{113} 1092^{56} \equiv_{113} 1$$

hence, the order of 2 mod 113 is at least 56 and therefore not a prime generator.

11.2

using lagrange's theorem, the order of 3 must divide $\phi(n)$

$$3^{56} \equiv_{113} 112$$
$$3^{16} \equiv_{113} 16$$

if the order of 3 was anything but $\phi(n)$ one of congruences would have been congruent to 1
hence the order of 3 modulus 113 is $\phi(113)$ or 112