1.

$$257 \overline{)30030} \quad 116$$
$$257$$
$$433$$
$$257$$
$$1760$$
$$1542$$
$$218$$

$$218 \overline{)257} \quad 1$$
$$218$$
$$39$$

$$39 \overline{)218} \quad 5$$
$$195$$
$$23$$

$$23 \overline{)39} \quad 1$$
$$23$$
$$16$$

$$16 \overline{)23} \quad 1$$
$$16$$
$$7$$

$$7 \overline{)16} \quad 2$$
$$14$$
$$2$$

$$2 \overline{)7} \quad 3$$
$$6$$
$$1$$

$$\gcd(30030, 257) = 1$$

(2) 30030 and 257 are relatively prime.

$30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$

Let $\Phi = \{2, 3, 5, 7, 11, 13\}$

if 257 is composite, it must have a factor c, s.t., $c \leq \sqrt{257}$

All candidates for c are either in Φ or multiples of elements of Φ, namely 2...16
Since $17^2 > 257$

None of those divide 257
since $\gcd(30030, 257) = 1$

So 257 is prime

3 Fermat's little theorem

if p is prime and a an integer

s.t. $p \nmid a$

$$a^{p-1} \equiv 1 \bmod p$$

Find $2^{58} \pmod{11}$

11 is prime and $11 \nmid 2$

So $2^{10} \equiv 1 \bmod 11$

$$2^{58} \equiv (2^{10})^5 2^8 \equiv 2^8 \bmod 11$$

$$\equiv 3 \bmod 11$$

4. $enc(x) = (\alpha x + \beta) \bmod 26$

Derive dec.

Decryption is the inverse of encryption

Do Let $y = (\alpha x + \beta) \bmod 26$

and Solve for x

$y = (\alpha x + \beta) \bmod 26$

$\alpha x = (y - \beta) \bmod 26$

Define α^{-1}, where α^{-1} is an integer and $\alpha\alpha^{-1} = 1$

α^{-1} exists mod 26 only if $\gcd(\alpha, 26) = 1$

As long as we restrict α to ~~odd~~ integers in the range $[1..25]$ excluding 13, α^{-1} exists.

$\alpha^{-1}\alpha = \alpha^{-1}(y - \beta) \bmod 26$

$\alpha = \alpha^{-1}y - \alpha^{-1}\beta \bmod 26$

$\Rightarrow$

$dec(x) = (\alpha^{-1}y) + (-\alpha^{-1}\beta) \bmod 26$

5. Find Keyspace of the Vignere cipher

A cipher consists of 3 parts

1. KeyGen
2. Encrypt
3. Decrypt

Only keyGen is necessary for this problem

Randomly generate a vector, V, of N integers each in the range [0, 25]

$V = [B_1, B_2, \ldots, B_N]$

where there are 26 possibilities for each B_k

Keyspace = 26^N where N is the length of the key

~~7.~~ 6. Find the last three digits of 7^{803}

Finding last 3 digits is the same as working mod 1000

Problem may be restated)
Find $7^{803} \mod 1000$

Since
$$\gcd(7, 1000) = 1$$

Eulers will be used
for any integers a, n
if $\gcd(a, n) = 1$
$$a^{\phi(n)} \equiv 1 \mod n$$

So $7^{\phi(1000)} \equiv 1 \mod n$

$$\phi(1000) = \phi(2^3 \cdot 5^2) = \phi(2^3)\,\phi(5^2)$$
$$= 2^3(1 - 1/2) \cdot 5^2(1 - 1/5)$$
$$= 4 \cdot 100$$
$$= 400$$
$$7^{400} \equiv 1 \mod 1000$$

$$7^{803} = 7^{(400)^2 \cdot 7^3}$$
$$\equiv 1 \cdot 7^3 \mod 1000$$
$$\equiv 343 \mod 1000$$

Last 3 digits of 7^{803} are $\underline{\underline{343}}$

7. Find $2^{43210} \mod 101$

Format

if p is prime and a an integer s.t $p \nmid a$

$$a^{p-1} \equiv 1 \mod p$$

$$2^{100} \equiv 1 \mod 101$$

$$2^{43210} = 2^{(100)^{432}} \cdot 2^{10}$$

$$\equiv 1 \cdot 2^{10} \mod 101$$

$$\equiv 2^{10} \mod 101$$

$$\equiv 14 \mod 101$$

8 Prove $1835^{1910} + 1986^{2061} \equiv 0 \mod 7$

Fermat if p is prime $\nmid a$ $a^{p-1} \equiv 1 \mod p$

(A) $1835^{6} \equiv 1 \mod 7$

$1885^{1910} = 1835^{1908} \; 1835^{2}$

$= (1835^{6})^{318} \; 1835^{2}$

$\equiv 1835^{2} \mod 7$

$\equiv 5^{2} \cdot 367^{2} \mod 7$

$\equiv 4 \cdot 367^{2} \mod 7$

$\equiv 4 \cdot 9 \mod 7$

$\equiv 1 \mod 7$

(B)

$1986^{6} \equiv 1 \mod 7$

$1986^{2061} = 1986^{2058} \cdot 1986^{3} \mod 7$

$\equiv$

$\equiv 1986^{(6)^{343}} \cdot 1986^{3} \mod 7$

$\equiv 1986^{3} \mod 7$

$\equiv 2^{3} \cdot 3^{3} \cdot 331^{3} \mod 7$

$\equiv 6 \mod 7$

So

$(1835^{1910} + 1986^{2061}) \equiv (1+6) \equiv 0 \mod 7$

9. Evaluate

$$2^{100000} \mod 77$$

For any integers a, n with $\gcd(a,n)=1$, $n \geq 1$

$$a^{\phi(n)} \equiv 1 \mod n$$

$\gcd(2,77) = 1$ $\quad 77 \geq 1$

$\phi(77) = \phi(7 \cdot 11) = \phi(7) \cdot \phi(11)$

both 7 and 11 are prime

$\phi(7) = 7\left(1 - \frac{1}{7}\right) = 7 - 1 = 6$

$\phi(7) \cdot \phi(11) = 60$

$$2^{60} \equiv 1 \mod n$$

$$2^{100000} = 2^{40} \cdot 2^{(60)1666}$$
$$\equiv 2^{40} \mod 77$$
$$\equiv (2^{10})^4 \mod 77$$
$$2^8 \equiv 61 \mod 77$$
$$\equiv (23)^4 \mod 77$$
$$\equiv (67)^2 \mod 77$$
$$\equiv 23 \mod 77$$

10 3 to a row, $r=1$
4 to a row, $r=2$
5 to a row, $r=3$
} how many people are needed

Restated in terms of the CRT

$$x \equiv 1 \bmod 3$$
$$\equiv 2 \bmod 4$$
$$\equiv 3 \bmod 5$$

By the Chinese Remainder theorem

$$n = 3 \cdot 4 \cdot 5 = 60 = n_1 n_2 n_3$$

$$N_1 = \frac{60}{n_1} = \frac{60}{3} = 20$$

$$N_2 = \frac{60}{n_2} = \frac{60}{4} = 15$$

$$N_3 = \frac{60}{n_3} = \frac{60}{5} = 12$$

$$20 \cdot x_1 \equiv 1 \bmod 3$$
$$15 \cdot x_2 \equiv 1 \bmod 4$$
$$12 \cdot x_3 \equiv 1 \bmod 5$$

Find X_1 which is $20^{-1} \bmod 3$

X_2 " " $15^{-1} \bmod 4$

X_3 " " $12^{-1} \bmod 5$

By Euler

if $n \geq 1$ and $\gcd(a,n) = 1$

$$a^{\phi(n)-1} \equiv a^{-1} \bmod n$$

X_1 $\gcd(20,3) = 1$ $\phi(3) = 2$

$$X = 20^{-1} \equiv 20^{2-1} \bmod 3$$
$$\equiv 2 \bmod 3$$

X_2 $\gcd(15,4) = 1$ $\phi(4) = 2$

$$X_2 \equiv 15^{-1} \equiv 15 \bmod 4$$
$$\equiv 3 \bmod 4$$

X_3 $\gcd(12,5) = 1$ $\phi(12) = \phi(3) \cdot \phi(4) = 4$

$$X_3 \equiv 12^{-1} \equiv 12^3 \bmod 5$$
$$\equiv 3 \bmod 5$$

$$X = (a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3) \bmod n$$

$a_1 = 1 \quad N_1 = 20 \quad x_1 = 2$

$a_2 = 2 \quad N_2 = 15 \quad x_2 = 3$

$a_3 = 3 \quad N_3 = 12 \quad x_3 = 3$

$n = 60$

$$X = (1 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3) \bmod 60$$

$$= (40 + 90 + 108) \bmod 60$$

$$= 238 \bmod 60$$

$$= \boxed{58}$$

Next smallest number must satisfy CRT. Call it p

$p \equiv 58 \bmod 60$

$p - 58 = 60k$

$p = 58 + 60k$

$k = 1$ is the smallest k s.t. $p > 58$

So $p = 58 + 60 = \boxed{118}$

Notice

$118 \equiv 1 \bmod 3$

$118 \equiv 2 \bmod 4$

$118 \equiv 3 \bmod 5$