Exercises:

1. Compute $\phi(50910363)$ knowing that

$$50910363 = 3^4 \times 7^2 \times 101 \times 127.$$

$$\phi(50910363) = (3^4-3^3)(7^2-7)(101-1)(127-1)$$

2. Use your answer from the previous question to compute

$$= 28576800$$

$$2^{28576807} \ mod \ \underbrace{50910363}_{m}.$$

3. Compute 3^{999} mod 143. $= 13 \cdot 11$

$$\phi(143) = (13-1)(11-1) = 120$$

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

$$2^{28576800+7} \equiv 2^{28576800} \, 2^7 \pmod{50910363}$$

$$\equiv 2^7 \pmod{50910363}$$

$$\equiv 128 \pmod{50910363}$$

$$3^{999} \equiv 3^{960+39} \equiv 3^{8 \cdot 120} \cdot 3^{39}$$

$$\equiv (3^{120})^8 \, 3^{39} \equiv 3^{39} \pmod{143}$$

$$(\text{mod } 143)\quad 3^{39} \equiv 3^{1}\cdot 3^{38} \equiv 92$$

$$(\text{mod } 143)\quad 3^{38} \equiv \left(3^{19}\right)^{2} \equiv 126$$

$$3^{19} \equiv 3^{1}\cdot 3^{18} \equiv 3^{4} \equiv 81$$

$$3^{18} \equiv \left(3^{9}\right)^{2} \equiv 27 \equiv 3^{3}$$

$$3^{9} \equiv 3^{1}\cdot 3^{8} \equiv 92$$

$$3^{8} \equiv \left(3^{4}\right)^{2} \equiv 126$$

$$3^{4} \equiv 81$$

$$\boxed{\begin{aligned} 3^{18} &\equiv 3^{3} \quad (\text{mod } 143) \\ 3^{15} &\equiv 1 \quad (\text{mod } 143) \end{aligned}}$$

$$3^{39} \equiv 3^{2\cdot 15+9} \equiv \left(3^{15}\right)^{2}\cdot 3^{9} \quad (\text{mod } 143)$$

$$\equiv 3^{9}$$

$m = 350123 = 347 \cdot 1009$

$\phi(m) = 346 \cdot 1008 = 348768$

$e = 37$ want $d = ?$

$ed \equiv 1 \pmod{348768}$

$348768 = 9426 \cdot 37 + 6 \Rightarrow 6 = 348768 - 9426 \cdot 37$

$37 = 6 \cdot 6 + 1$

$1 = 37 - 6 \cdot 6$

$= 37 - 6(348768 - 9426 \cdot 37)$

$= (6 \cdot 9426 + 1) \cdot 37 - 6 \cdot 348768$

$1 \equiv (6 \cdot 9426 + 1) \cdot 37 \pmod{348768}$

$1 \equiv \underbrace{56557}_{d} \cdot 37 \pmod{348768}$

$m = 143 \qquad \phi(m) = 120$

$m+1-\phi(m) = 144-120 = 24$

$$p = \frac{24 + \sqrt{24^2 - 4\cdot 143}}{2} = \frac{24+\sqrt{576-572}}{2}$$

$$= \frac{24+2}{2} = 13$$

$$q = \frac{24 - \sqrt{24^2 - 4\cdot 143}}{2} = \frac{24-\sqrt{576-572}}{2}$$

$$= \frac{24-2}{2} = 11$$

$\cancel{(x-11)(x-13) = x-24}$

Quadratic Sieve Factoring Algorithm

1. Pick random $a \in \{1, 2, \ldots, (m-1)/2\}$

2. If $gcd(a, m) > 1$ then DONE!

3. Otherwise compute $a^2 \bmod m$ and compare to other squares already computed. If there is another number $b \neq a$ such that
$$a^2 \equiv b^2 \mod m$$
then
$$(a+b)(a-b) = a^2 - b^2 \equiv 0 \mod m$$
This means that
$$(a+b)(a-b) = km$$
for some k. Since both $a+b$ and $a-b$ are less than m, m cannot divide either one. Therefore
$$m = gcd(m, a+b) \times gcd(m, a-b)$$

m won't divide a+b & a−b because m > a+b & a−b

but m divides their product since p·q divides (a+b)(a−b)
⇒ p = gcd(a+b, m) & q = gcd(a−b, m)

Quadratic Sieve

Example: $m = 91$

a	19	1	23	18	2	24	16
a^2	88	1	74	51	4	30	74

$$\begin{aligned} 91 &= gcd(91, \overset{39}{23+16}) \times gcd(91, 23-16) \\ &= gcd(91, 39) \times gcd(91, 7) \\ &= 13 \times 7 \end{aligned}$$

$91 = 2 \cdot 39 + 13 \quad gcd(91, 39) = 13$

$91 = 13 \cdot 7$

1. given m, find $\phi(m)$

2. given a, k, m find

$$a^k \pmod{m}$$

(a) use given information to simplify your calculation.

3. Given a, m s.t. $\gcd(a,m)=1$ find b s.t. $a \cdot b \equiv 1 \pmod{m}$

4. Given a, b, m solve equation of the form $ax \equiv b \pmod{m}$

5. given $\underset{\substack{\shortparallel \\ p \cdot q}}{m}$ & $\phi(m)$ factor m

6. be able to convert messages to numbers and back using base 26

7. given a, b & m s.t. $a^2 \equiv b^2 \pmod{m}$ factor m