

1. A method was devised by Fermat to test for prime numbers. We have observed that

$$2^2 - 1 = 3; \quad 2^{12} - 1 = 4095 = 13 \times 315.$$

More generally, **Fermat's 'little' theorem** says that *if  $p$  is a prime and the integer  $a$  satisfies  $0 < a < p$ , then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

That is,  $a^{p-1} - 1$  is divisible by  $p$ .

Consider the following 'proof' of Fermat's little theorem.

"List the first  $p - 1$  positive multiples of  $a$ :

$$a, 2a, 3a, \dots, (p-1)a.$$

Suppose that

$$ra \equiv c \pmod{p} \quad \text{and} \quad sa \equiv c \pmod{p},$$

where  $r, s$  and  $c$  are positive integers less than  $p$ , then (because  $p$  does not divide  $a$  and  $p$  is a prime)  $r = s$ . Therefore

$$\begin{aligned} a &\equiv c_1 \pmod{p}, \\ 2a &\equiv c_2 \pmod{p}, \\ &\cdot \\ &\cdot \\ (p-1)a &\equiv c_{p-1} \pmod{p}, \end{aligned}$$

where  $c_1, c_2, \dots, c_{p-1}$  are *distinct* positive integer, all of them less than  $p$ . It follows that, in some order, they are  $1, 2, \dots, p-1$ . We have

$$\begin{aligned} &a \times 2a \times 3a \cdots \times (p-1)a \\ &\equiv c_1 \times c_2 \times c_3 \cdots \times c_{p-1} \pmod{p} \\ &\equiv 1 \times 2 \times 3 \cdots \times (p-1) \pmod{p} \quad (\text{after rearranging the terms}). \end{aligned}$$

That is,

$$(a^{p-1}) \times 1 \times 2 \times 3 \cdots \times (p-1) \equiv 1 \times 2 \times 3 \cdots \times (p-1) \pmod{p},$$

which implies that  $a^{p-1} \equiv 1 \pmod{p}$ . End of the proof."

Critically evaluate the above 'proof' and decide whether it is correct or not. If you think that it is incorrect, how would you 'repair' the proof?

2. Consider the exquisite Rivest-Shamir-Adleman (**RSA**) algorithm for the open key encryption. First, generate two prime numbers, say,

$$p = 7 \quad \& \quad q = 19$$

(in practice they are much larger). Let

$$n = pq = 133 \quad \& \quad k = (p - 1)(q - 1) = 6 \times 18 = 108.$$

Take  $e = 5$  and  $d = 65$  so that

$$ed = 325 \equiv 1 \pmod{108} \quad (\text{as } 325 = 3 \times 108 + 1).$$

(a) Both  $(133, 5)$  and  $(133, 65)$  can be used as the public key. Why do you think it is better to put  $e = 5$  as the public key and keep  $d = 65$  private?

Suppose that the message we send out is represented by the integer  $m = 6$ . The cipher  $c$  is generated by

$$m^e \equiv c \pmod{n} \implies 6^5 = 7776 \equiv c \pmod{133} \implies c = 62.$$

(b) Explain why it is hard to ascertain  $x$  from the modulo equation

$$x^5 \equiv 62 \pmod{133}.$$

(c) By a direct calculation using modulo arithmetic, show that  $(62)^{65} \equiv 6 \pmod{133}$ .

(d) Repeat the process by using  $n = 133$  and  $d = 65$  as the public key. (Again, take  $m = 6$ .)