1. Using RSA with public key $(34, 3)$,

   (a) encrypt ***MATH***,

   (b) decrypt the message:

$$\mathbf{10\ 9\ 16\ \mid\ 25\ 23\ 27\ 18\ 23\ 10}.$$

Solution.

(a) Translating from the English alphabet we have

$$\begin{array}{ccc} \boldsymbol{A} & \longrightarrow & \mathbf{1} \\ \boldsymbol{H} & \longrightarrow & \mathbf{8} \\ \boldsymbol{M} & \longrightarrow & \mathbf{13} \\ \boldsymbol{T} & \longrightarrow & \mathbf{20}. \end{array}$$

To encrypt we must calculate

$$\begin{aligned} c_A &= 1^3 \equiv \mathbf{1} \mod 34 \\ c_H &= 8^3 \equiv \mathbf{2} \mod 34 \\ c_M &= 13^3 = 13 \cdot 256 \equiv 13 \cdot 18 = 234 \equiv \mathbf{30} \mod 34 \\ c_T &= 20^3 = 20 \cdot 400 \equiv 20 \cdot 26 = 520 \equiv \mathbf{10} \mod 34 \end{aligned}$$

and the encrypted message is thus

$$\mathbf{1\ 2\ 30\ 10}.$$

(b) Since $\varphi(34) = 16$ and $3 \cdot 11 = 33 = 1 + 2 \cdot 16$ we can choose $d = 11$. Now, according to RSA decryption

$$\begin{aligned} m_{10} &= 10^{11} = 100^5 \cdot 10 \equiv (-2)^5 \cdot 10 = -32 \cdot 10 \equiv 20 \mod 34 \\ m_9 &= 9^{11} = 81^5 \cdot 9 \equiv 13^5 \cdot 9 = 169^2 \cdot 117 \equiv (-1)^2 \cdot 15 = 15 \mod 34 \\ m_{16} &= 16^{11} = 256^5 \cdot 16 \equiv 18^5 \cdot 16 = 324^2 \cdot 18 \cdot 16 \equiv 18^2 \cdot 288 \equiv 18 \cdot 16 \\ &\equiv 16 \mod 34. \end{aligned}$$

In the same way,

$$\begin{aligned} m_{25} &= 25^{11} = 19 \mod 34 \\ m_{23} &= 23^{11} = 5 \mod 34 \\ m_{27} &= 27^{11} = 3 \mod 34 \\ m_{18} &= 18^{11} = 18 \mod 34 \end{aligned}$$

and

$$m_{10} = 10^{11} = 20 \mod 34,$$

which by looking at the letter equivalence gives

$$\mathbf{10\ 9\ 16} \ \mid\ \mathbf{25\ 23\ 27\ 18\ 23\ 10} \equiv \textbf{\textit{TOP}} \mid \textbf{\textit{SECRET}}. \qquad \square$$

---

2. (a) Prove that if $n > 4$ is composite then

$$(n-1)! \equiv 0 \mod n.$$

(b) Compute $2^{322} \mod 323$ and conclude from Fermat's little theorem that 323 is not prime.

Solution.

(a) Since n is composite, we can write $n = d \cdot d^*$ for some integers $1 < d < \bar{d} \leq n-1$ unless $n = p^2$ for some prime p (prove this!). In the first case, both d and d^* appear as factors in $(n-1)! = (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1$ and therefore $n \mid (n-1)!$. In the latter, since $n > 4$, we must have $p > 2$ and so $p, 2p \leq n-1$ appear as factor in $(n-1)!$ proving again that $n \mid (n-1)!$.

(b) By successive division (as when one wants to find the binary expression of $322 =$ "$323 - 1$"), since

i	q	r_i	$2^{2^i} \mod 323$
0	322	0	2
1	161	1	4
2	80	0	16
3	40	0	256
4	20	0	290
5	10	0	120
6	5	1	188
7	2	0	137
8	1	1	35

we have,

$$2^{322} = 2^{2^8 + 2^6 + 2} = 2^{2^8} \cdot 2^{2^6} \cdot 2 = 4 \cdot 188 \cdot 35 = 157 \mod 323$$

and hence, by Fermat's little theorem, $n = 323$ is not prime (otherwise we should have $2^{322} \equiv 1 \mod 323$). In fact $323 = 17 \cdot 19$. $\square$

---

3. Find rules of divisibility of an integer by 5, 9 and 11, and prove each of those rules using modular arithmetic.

   Solution. Let $n = a_m a_{m-1} \cdots a_1 a_0$ be the decimal expansion of a positive integer n. This means that

$$n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$$

with $0 \le a_0, a_1, \ldots, a_{m-1}, a_m \le 9$ and $a_m \neq 0$. Since

$$\begin{aligned} 10^k &\equiv 0 \mod 5 \\ 10^k &\equiv 1 \mod 9 \end{aligned}$$

and

$$10^k \equiv (-1)^k \mod 11 = \begin{cases} 1, & \text{if } k \text{ is even} \mod 11 \\ -1, & \text{if } k \text{ is odd} \mod 11 \end{cases}$$

for $k = 1, 2, \ldots, m$, we have

$$\begin{aligned} n &\equiv a_0 \mod 5 \\ n &\equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \mod 9 \end{aligned}$$

and

$$\begin{aligned} n &\equiv (-1)^m a_m + (-1)^{m-1} a_{m-1} + \cdots - a_1 + a_0 \\ &= \sum_{\substack{0 \le i \le m \\ i \text{ even}}} a_i - \sum_{\substack{0 \le i \le m \\ i \text{ odd}}} a_i \mod 11. \end{aligned}$$

Therefore the rules read as follows:

- An integer is divisible by 5 if its last digits is a 0 or a 5.
- An integer is divisible by 9 if the sum of its digits a multiple of 9.
- An integer is divisible by 11 if the difference between the sum of its even and odd numbered digits is a multiple of 11. □

---

4. Suppose m and n are relatively prime positive integers

   (a) Show that if some a integer $m \mid a$ and $n \mid a$ then $m \cdot n \mid a$.

(b) Show that the map Ψ defined by

$$\begin{array}{ccc} \mathbb{Z}^*_{m\cdot n} & \xrightarrow{\Psi} & \mathbb{Z}^*_m \times \mathbb{Z}^*_n \\ [a]_{m\cdot n} & \hookrightarrow & ([a]_m, [a]_n) \end{array}$$

is a bijection.

(c) Conclude from (b) that Euler's φ function is multiplicative, i.e.,

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

Solution.

(a) If $m \mid a$ and $n \mid a$ these are integers q_m and q_n such that

$$a = m \cdot q_m = n \cdot q_n.$$

Hence $n \mid m \cdot q_m$ and since $\gcd(m, n) = 1$ it follows that $n \mid q_m$. Thus, for some integer κ, $q_m = n \cdot \kappa$ and therefore

$$a = m \cdot n \cdot \kappa$$

which means that $m \cdot n \mid a$.

(b) First observe that Ψ is well defined, for if $\gcd(a, m \cdot n) = 1$ then $\gcd(a, m) = \gcd(a, n) = 1$ also. Next we will show that Ψ is one-to-one and onto.

- Ψ is one-to-one. If $[a]_{m\cdot n}, [b]_{m\cdot n} \in \mathbb{Z}^*_{m\cdot n}$ and

$$\Psi\big([a]_{m\cdot n}\big) = \Psi\big([b]_{m\cdot n}\big)$$

then

$$\left.\begin{array}{r} [a]_m = [b]_m \\ [a]_n = [b]_n \end{array}\right\} \underset{\text{by } (a)}{\overset{}{\underset{\uparrow}{\Rightarrow}}} \; n \mid (b-a) \text{ and } m \mid (b-a) \Rightarrow m\cdot n \mid (b-a).$$

This means that $[a]_{m\cdot n} = [b]_{m\cdot n}$ as we wanted to show.

- Ψ is onto. Let $[\alpha]_m \in \mathbb{Z}^*_m$ and $[\beta]_m \in \mathbb{Z}^*_n$ and choose $1 \le a < m \cdot n$ such that

$$\left.\begin{array}{l} a \equiv \alpha \mod m \\ a \equiv \beta \mod n \end{array}\right\} \qquad (*)$$

as given by the Chinese remainder theorem. Since $\gcd(\alpha, m) = \gcd(\beta, n) = 1$ we have that $\gcd(a, m \cdot n) = 1$ and hence $[a]_{m\cdot n} \in \mathbb{Z}^*_{m\cdot n}$ and, by (*), $\Psi\big([a]_{m\cdot n}\big) = \big([\alpha]_m, [\beta]_n\big)$.

(*c*) Since

$$\varphi(m) :\ = \# \left\{1 \leq k \leq n \ / \ \gcd(k, m) = 1\right\} = \#\mathbb{Z}_m^*,$$

by (*b*) we have

$$\varphi(m \cdot n) = \#\mathbb{Z}_{m \cdot n}^* \underset{\substack{\uparrow \\ \Psi \text{ bijective}}}{=} \#\mathbb{Z}_m^* \times \mathbb{Z}_n^* = \varphi(m) \cdot \varphi(n). \qquad \square$$

---

5. Let φ be Euler's function.

(*a*) Show that if a and $m > 1$ are relatively prime positive integers, then the inverse of a modulo m is $a^{\varphi(m)-1}$.

(*b*) Use (*a*) to find

(*i*) the inverse of 4 modulo 9,

(*ii*) the inverse of 5 modulo 8.

Solution.

(*a*) By the analog to Fermatt's little theorem we know that if a and m are relatively prime then $a^{\varphi(m)} \equiv 1 \mod m$. But then,

$$[a]_m \cdot [a^{\varphi(m)-1}]_m = [a^{\varphi(m)-1}]_m \cdot [a]_m = [a^{\varphi(m)}]_m = [1]_m$$

which just means that $a^{\varphi(m)-1}$ is the inverse of a modulo m.

(*b*) (*i*) Since $\varphi(9) = \varphi(3^2) = 3 \cdot 2 = 6$,

$$[4]_9^{-1} = [4^5]_9 = [16^2 \cdot 4]_9 = [(-2)^2 \cdot 4]_9 = [16]_9 = [7]_9.$$

(*ii*) Now $\varphi(8) = \varphi(2^3) = 4$ and hence

$$[5]_8^{-1} = [5^3]_8 = [25 \cdot 5]_8 = [1 \cdot 5]_8 = [5]_8. \qquad \square$$