MATH 220
DISCRETE MATHEMATICS AND CRYPTOGRAPHY

Tutorial 4 **Solutions**

1. Now $1001 = 7 \times 11 \times 13$ (prime factorisation), so

$$\phi(1001) = (7-1)(11-1)(13-1) = 720.$$

Similarly, $1000 = 2^3 \times 5^3$, so

$$\phi(1000) = (2^3 - 2^2)(5^3 - 5^2) = 400.$$

2. Let

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

so that

$$n^m = p_1^{m\alpha_1} p_2^{m\alpha_2} \cdots p_k^{m\alpha_k}$$

and

$$\phi(n^m) = \left(p_1^{m\alpha_1} - p_1^{m\alpha_1 - 1}\right)\left(p_2^{m\alpha_2} - p_2^{m\alpha_2 - 1}\right) \cdots \left(p_k^{m\alpha_k} - p_k^{m\alpha_k - 1}\right).$$

Now take out a factor of the form $p_i^{(m-1)\alpha_i}$ from each product term on the right. Then

$$\begin{aligned}\phi(n^m) &= p_1^{(m-1)\alpha_1} p_2^{(m-1)\alpha_2} \cdots p_k^{(m-1)\alpha_k} \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) \\ &= n^{m-1}\phi(n)\end{aligned}$$

as required.

3. By the previous question,

$$\phi(1000) = \phi(10^3) = 10^2\phi(10) = 10^2\phi(5 \times 2) = 10^2 \times 4 \times 1 = 400.$$

4. Now $110 = 64 + 32 + 8 + 4 + 2$. Next calculate

$$\begin{aligned} 9^1 &\equiv 9 \bmod 19 \\ 9^2 &\equiv 81 \equiv 5 \bmod 19 \\ 9^4 &\equiv 25 \equiv 6 \bmod 19 \\ 9^8 &\equiv 36 \equiv 17 \bmod 19 \\ 9^{16} &\equiv 289 \equiv 4 \bmod 19 \\ 9^{32} &\equiv 16 \bmod 19 \\ 9^{64} &\equiv 256 \equiv 9 \bmod 19 \end{aligned}$$

Therefore

$$\begin{aligned}9^{110} &= 9^{64} \times 9^{32} \times 9^{8} \times 9^{4} \times 9^{2} \\ &\equiv 9 \times 16 \times 17 \times 6 \times 5 \bmod 19 \\ &\equiv 5 \bmod 19\end{aligned}$$

Fermat's Little Theorem says that

$$9^{18} \equiv 1 \bmod 19.$$

Since $110 = 18 \times 6 + 2$,

$$\begin{aligned}9^{110} &= \left(9^{18}\right)^{6} \times 9^{2} \\ &\equiv 9^{2} \bmod 19 \\ &\equiv 5 \bmod 19\end{aligned}$$

5. Taking powers of 2 mod 11 gives

$$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 5,\ 2^5 = 10,\ 2^6 = 9,\ 2^7 = 7,\ 2^8 = 3,\ 2^9 = 6,\ 2^{10} = 1.$$

From this, we can write out the discrete log table as

a	$\mathrm{dlog}_2\, a$
1	10
2	1
3	8
4	2
5	4
6	9
7	7
8	3
9	6
10	5

It is easily checked that 3 is not a generator for $\mathbb{Z}_{11}^*$. For example, $3^x \equiv 7 \bmod 11$ has no solution, and therefore $\mathrm{dlog}_3\, 7$ is not defined in $\mathbb{Z}_{11}$.

6. (a) In the RSA scheme, if e is the *exponent* and n the *modulus*, then m encrypts to c where

$$c \equiv m^e \bmod n.$$

So, in this case with $e = 3$ and $n = 12091$, $m = 2107$ encrypts to

$$\begin{aligned}c &\equiv 2107^3 \bmod 12091 \\ &= 7077\end{aligned}$$

(b) Since $n = 12091 = 107 \times 113$ as a product of primes, the decryption key is the pair of primes $\{107, 113\}$.

Alternatively, you could say that it is $d = e^{-1}$ in $\mathbb{Z}_{\phi(n)}$, which can be calculated when you know the primes 107 and 113.

(c) To decrypt c back to m,

$$m \equiv c^d \bmod n,$$

where d is the inverse of e in $\mathbb{Z}_{\phi(n)}$.

In this case, $n = 12091 = 107 \times 113$. So $\phi(n) = 106 \times 112 = 11872$.

Since $e = 3$, we can apply Euclid's Algorithm to find 3^{-1} in $\mathbb{Z}_{11872}$.

$$11872 = 3 \times 3957 + 1$$

so $d = 3^{-1} = -3957 = 7915$ in $\mathbb{Z}_{11872}$.

Finally, if $c = 9812$, then c decrypts to

$$\begin{aligned} m &\equiv 9812^{7915} \bmod 12091 \\ &= 142 \end{aligned}$$

(A quick way to calculate powers in modular arithmetic is to use the Maple command `n\&^k mod m;` which calculates, very efficiently, $n^k \bmod m$.)

7. Public modulus is $pq = 47233$. The decryption exponent d satisfies

$$ed \equiv 1 \bmod \phi(n),$$

where $e = 71$ and $\phi(n) = (149 - 1)(317 - 1) = 46768$. After a little work using Euclid's Algorithm, we get $d = 28983$.

8. Since e_1 and e_2 are relatively prime, that is $\gcd(e_1, e_2) = 1$, it follows by Euclid's Algorithm that Eve can find integers x and y such that

$$xe_1 + ye_2 = 1.$$

But then

$$\begin{aligned} (c_1)^x \cdot (c_2)^y &\equiv (m^{e_1})^x \cdot (m^{e_2})^y \bmod n \\ &\equiv m^{xe_1 + ye_2} \bmod n \\ &\equiv m^1 \bmod n \\ &\equiv m \bmod n \end{aligned}$$

Thus, as Eve knows e_1, e_2, x, y, n, Eve knows $m \equiv (c_1)^x \cdot (c_2)^y \bmod n$.

9. First, we know the factors of $n = 713$, in particular, $713 = 23 \times 31$. (Recall that we start by choosing two primes to get n so factorisation is not an issue in practice.)

Let $p = 23$ and $q = 31$. We next have to find the square roots of $c = 200 \bmod p$ and mod q.

$$\begin{aligned} m_p^2 &\equiv 200 \bmod 23 \\ &\equiv 16 \bmod 23 \end{aligned}$$

So

$$m_p \equiv \pm 4 \bmod 23$$

giving $m_p = 4$ or $m_p = 19$.

Similarly,

$$\begin{aligned} m_q^2 &\equiv 200 \bmod 31 \\ &\equiv 14 \bmod 31 \end{aligned}$$

giving $m_q = 13$ or $m_q = 18$ (from the hint).

We now need to find u and v such that $pu + qv = 1$, that is, $23u + 31v = 1$. Using Euclid's Algorithm, we obtain a solution $u = -4$ and $v = 3$.

Finally, we calculate the four numbers $\pm pum_q \pm qvm_p \bmod n$. That is,

$$\begin{aligned} \pm(23)(-4)(13) \pm (31)(3)(4) &\equiv \pm 1196 \pm 372 \bmod 713 \\ &\equiv 1568, 824, -1568, -824 \bmod 713 \\ &\equiv 142, 111, 571, 602 \bmod 713 \end{aligned}$$

These are the four possible messages.

10. (a) m is encrypted to

$$\begin{aligned} c &\equiv m^2 \bmod n \\ &\equiv 17^2 \bmod 65 \\ &\equiv 289 \bmod 65 \\ &\equiv 29 \bmod 65, \end{aligned}$$

so $c = 29$.

(b) First we need to calculate

$$m_p \equiv \sqrt{c} \bmod 5$$

and

$$m_q \equiv \sqrt{c} \bmod 13$$

with $c = 29$.

This means that we have to solve the equations

$$\begin{aligned} m_p^2 &\equiv 29 \bmod 5 \\ &\equiv 4 \bmod 5 \end{aligned}$$

and

$$\begin{aligned} m_q^2 &\equiv 29 \bmod 13 \\ &\equiv 3 \bmod 13. \end{aligned}$$

Running through the possibilities, gives $m_p = 2$ and $m_q = 4$.

Second, we need to find integers u and v such that $5u + 13v = 1$. We can either guess or use Euclid's Algorithm as follows:

$$\begin{aligned} 13 &= 2 \times 5 + 3 \\ 5 &= 1 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \end{aligned}$$

Working backwards,

$$\begin{aligned} 1 &= 3 - 1 \times 2 \\ &= 3 - 1 \times (5 - 1 \times 3) = 2 \times 3 - 1 \times 5 \\ &= 2 \times (13 - 2 \times 5) - 1 \times 5 \\ &= 2 \times 13 - 5 \times 5. \end{aligned}$$

So we can take $u = -5$ and $v = 2$. (Note that other solutions exist, for example, $u = 8$ and $v = -3$. The general solution is of the form

$$\begin{aligned} u &= -5 + 13t \\ v &= 2 - 5t, \end{aligned}$$

where $t \in \mathbb{Z}$. The decryption does not depend on the choice of u and v.)

Finally, we calculate the four numbers

$$\pm p u m_q \pm q v m_p \bmod n,$$

that is,

$$\pm 5 \times (-5) \times 4 \pm 13 \times 2 \times 2 \bmod 65$$

or

$$\pm 100 \pm 52 \bmod 65$$

giving the four possible values for m as 17, 22, 43, and 48.

11. Suppose $a \equiv b \bmod n$. Then $a = b + kn$ for some $k \in \mathbb{Z}$. As $n = pq$, we have

$$a = b + k(pq),$$

and so $a = b + (kq)p$ and $a = b + (kp)q$. In turn, this implies

$$a \equiv b \bmod p$$

and

$$a \equiv b \bmod q.$$

We will prove the converse for when $p \neq q$. The proof for $p = q$ is similar. Suppose that $a \equiv b \bmod p$ and $a \equiv b \bmod q$. Then

$$a = b + kp \tag{1}$$

and

$$a = b + \ell q \tag{2}$$

for some $k, \ell \in \mathbb{Z}$.This implies that $kp = \ell q$, in particular $p \mid \ell q$. By Corollary 2.5, either $p \mid \ell$ or $p \mid q$. Since $p \neq q$, it follows that p does not divide q, and so $p \mid \ell$. Thus there is a $t \in \mathbb{Z}$ such that $pt = \ell$. Substituting into (2), we get

$$a = b + (pt)q = b + t(pq) = b + tn,$$

that is, $a \equiv b \bmod n$.

12. We first show that

$$\left(a^{\frac{p+1}{4}}\right)^2 \equiv a \bmod p.$$

Now

$$\left(a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p-1}{2}+1} \equiv \left(a^{p-1}\right)^{\frac{1}{2}} \cdot a^1 \equiv a \bmod p$$

as $a^{p-1} \equiv 1 \bmod p$ by Fermat's Little Theorem. Thus $a^{\frac{p+1}{4}}$ is a square root of $a \bmod p$. To see that $p - x$ is also a square root:

$$\left(p - \left(a^{\frac{p+1}{4}}\right)\right)^2 \equiv p^2 - 2p\left(a^{\frac{p+1}{4}}\right) + \left(a^{\frac{p+1}{4}}\right)^2 \equiv a \bmod p.$$