MATH 220

Discrete Mathematics and Cryptography

Tutorial 3 **Solutions**

---

1. (a) Working in $\mathbb{Z}_7$, trial and error gives $3 \times 2 = 6$, $3 \times 3 = 2$, $3 \times 4 = 5$, $3 \times 5 = 1$. So $3^{-1} \equiv 5 \bmod 7$.

(b) Working in $\mathbb{Z}_{11}$, we get $5 \times 2 = 10, 5 \times 3 = 4, \ldots, 5 \times 9 = 1$. So $5^{-1} \equiv 9 \bmod 11$.

2. (a)

$$\begin{aligned} 25 &= 21 + 4 \\ 21 &= 5 \times 4 + 1 \end{aligned}$$

and therefore

$$\begin{aligned} 1 &= 21 - 5 \times 4 \\ &= 21 - 5 \times (25 - 21) \\ &= 6 \times 21 - 5 \times 25 \end{aligned}$$

So, in $\mathbb{Z}_{25}$, $6 \times 21 = 1$, that is, $21^{-1} \equiv 6 \bmod 25$.

(b) Again,

$$\begin{aligned} 29 &= 2 \times 12 + 5 \\ 12 &= 2 \times 5 + 2 \\ 5 &= 2 \times 2 + 1 \end{aligned}$$

and therefore

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ &= 5 - 2 \times (12 - 2 \times 5) = 5 \times 5 - 2 \times 12 \\ &= 5 \times (29 - 2 \times 12) - 2 \times 12 \\ &= 5 \times 29 - 12 \times 12 \end{aligned}$$

So, in $\mathbb{Z}_{29}$, $-12 \times 12 = 1$, that is, $12^{-1} \equiv -12 \equiv 17 \bmod 29$.

3. The elements of Z_{12}^* are $1, 5, 7, 11$. The multiplication table is

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

and we can read off the inverses $1^{-1} = 1$, $5^{-1} = 5$, $7^{-1} = 7$, $11^{-1} = 11$.

4. (a) Since $2 \times 9 \equiv 1 \bmod 17$, we have $x \equiv 9 \bmod 17$. (Or, $x = 9 + 17k$ for some integer k.)

(b) The numbers are too large for trial and error (or a good guess), so we use Euclid's Algorithm to find $40^{-1} \bmod 1777$.

$$\begin{aligned} 1777 &= 44 \times 40 + 17 \\ 40 &= 2 \times 17 + 6 \\ 17 &= 2 \times 6 + 5 \\ 6 &= 1 \times 5 + 1 \end{aligned}$$

so $\gcd(1777, 40) = 1$. Work backwards to obtain

$$\begin{aligned} 1 &= 6 - 1 \times 5 \\ &= 6 - (17 - 2 \times 6) = 3 \times 6 - 1 \times 17 \\ &= 3(40 - 2 \times 17) - 17 = 3 \times 40 - 7 \times 17 \\ &= 3 \times 40 - 7(1777 - 44 \times 40) \\ &= 311 \times 40 - 7 \times 1777 \end{aligned}$$

Thus mod 1777, we have $311 \times 40 = 1$ or $40^{-1} \equiv 311 \bmod 1777$. So, from $40x \equiv 777 \bmod 1777$, we get

$$311 \times 40x \equiv 311 \times 777 \bmod 1777.$$

That is, $x \equiv 241647 \bmod 1777$ or $x \equiv 1752 \bmod 1777$. (Again this could be written as $x = 1752 + 1777k$ for some integer k.)

5. To solve the system

$$x + 2y \equiv 3 \bmod 7 \qquad (1)$$
$$3x + y \equiv 2 \bmod 7 \qquad (2)$$

of simultaneous equations for x and y, multiply (1) by 3 and subtract (2)

$$5y \equiv 0 \bmod 7$$

or $y \equiv 0 \bmod 7$. Substitute in (1), $x \equiv 3 \bmod 7$.

We can also write the solution in the form $x = 3 + 7k$, $y = 7l$, where k and l are integers.

6. To say that the method detects all single-digit errors means that if

$$7a_1 + 3a_2 + 9a_3 + 7a_4 + 3a_5 + 9a_6 + 7a_7 + 3a_8 + 9a_9 \equiv 0 \bmod 10 \qquad (3)$$

and one of the digits $a_1, a_2, \ldots, a_8$ is changed, the result will no longer be congruent to 0 mod 10.

Suppose to the contrary that, for example, a_1 is changed to b_1 and that as well as (3), we have

$$7b_1 + 3a_2 + 9a_3 + 7a_4 + 3a_5 + 9a_6 + 7a_7 + 3a_8 + 9a_9 \equiv 0 \bmod 10$$

Subtracting, gives

$$7(a_1 - b_1) \equiv 0 \bmod 10$$

Multiplying by 3 (which is 7^{-1} in $\mathbb{Z}_{10}$) gives

$$a_1 - b_1 \equiv 0 \bmod 10$$

and this is impossible since we are assuming that a_1 and b_1 are *different* integers in $\{0, 1, \ldots, 9\}$.

So any change in the first digit would be picked up as the check digit a_9 would no longer give (3).

Similar arguments hold for the other digits $a_2, a_3, \ldots, a_8$ because their coefficients are all relatively prime to 10.

Note. The coefficients 3, 7, 9 need only be odd numbers (except 5) for this single-digit check to work and we could even choose them all the same. In fact, this method detects quite a few more errors. For example, it detects most errors when two integers are transposed—a common enough error in practice. It will also detect many errors of the form $\cdots abc \cdots \to \cdots cba \cdots$.

7. The multiplication table for $\mathbb{Z}_{15}^*$ is

$\times$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

(a) From the table, we can read off inverses

$$1^{-1} = 1,\ 2^{-1} = 8,\ 4^{-1} = 4,\ 7^{-1} = 13,\ 8^{-1} = 2,\ 11^{-1} = 11,\ 13^{-1} = 7,\ 14^{-1} = 14.$$

(b)

$$\begin{array}{llll}
1^1 = 1 & & & \\
2^1 = 2, & 2^2 = 4, & 2^3 = 8, & 2^4 = 1 \\
4^1 = 4, & 4^2 = 1 & & \\
7^1 = 7, & 7^2 = 4, & 7^3 = 13, & 7^4 = 1 \\
8^1 = 8, & 8^2 = 4, & 8^3 = 2, & 8^4 = 1 \\
11^1 = 11, & 11^2 = 1 & & \\
13^1 = 13, & 13^2 = 4, & 13^3 = 7, & 13^4 = 1 \\
14^1 = 14, & 14^2 = 1 & &
\end{array}$$

So, the order of 1 is 1, the orders of 4, 11, 14 are 2 and the orders of 2, 7, 8, 13 are all 4.

(c) If $g^k = 1$, then $1 = g \times g^{k-1}$, and so g^{k-1} must be the inverse of g.

8. Suppose a is invertible. For each $\ell \in \{1, 2, \ldots\}$, consider a^ℓ in $\mathbb{Z}_m$. Let ℓ_1 and ℓ_2 be two distinct positive integers such that

$$a^{\ell_1} = a^{\ell_2}.$$

Since the number of elements in $\mathbb{Z}_m$ is finite, there has to be two such integers.

Without loss of generality, assume that $\ell_2 > \ell_1$. Now $a^{\ell_2} = a^{\ell_1}$, so, as a^{-1} exists,

$$\left(a^{-1}\right)^{\ell_1} a^{\ell_2} = \left(a^{-1}\right)^{\ell_1} a^{\ell_1} = 1.$$

Therefore,

$$\left(a^{-1}\right)^{\ell_1} a^{\ell_2} = a^{\ell_2 - \ell_1} = 1.$$

Choosing $k = \ell_2 - \ell_1$ completes the proof of this direction.

For the converse, suppose there is a positive integer k such that $a^k = 1$ in $\mathbb{Z}_m$. Then

$$a \cdot a^{k-1} = 1,$$

and so a^{-1} exists with $a^{-1} = a^{k-1}$.

9. Since $m - 1$ is non-zero and $(m-1)^2 = m^2 - 2m + 1 = 1$ in $\mathbb{Z}_m$, it follows that $m - 1$ is invertible and the order of $m - 1$ is 2. Therefore, by Theorem 3.13, we have that 2 divides $|\mathbb{Z}_m^*|$, so $|\mathbb{Z}_m^*|$ is even.

10. By Fermat's Little Theorem, $3^{72} \equiv 1 \bmod 73$, so

$$3^{75} \equiv 3^{72} \times 3^3 \equiv 1 \times 3^3 \equiv 27 \bmod 73.$$

11. If $p \mid a$, then $a \equiv 0 \bmod p$ and the result holds.

If p does not divide a, then, by Fermat's Little Theorem, $a^{p-1} \equiv 1 \bmod p$, and so

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

12.

$$\begin{aligned} 51 &= 38 \times 1 + 13 \\ 38 &= 13 \times 2 + 12 \\ 13 &= 12 \times 1 + 1 \end{aligned}$$

Working backwards,

$$\begin{aligned} 1 &= 13 - 12 \times 1 \\ &= 13 - (38 - 13 \times 2) \\ &= 13 \times 3 - 38 \\ &= (51 - 38) \times 3 - 38 \\ &= 51 \times 3 - 38 \times 4 \end{aligned}$$

Therefore $1 \equiv 38 \times -4 \bmod 51$. Since $-4 \equiv 47 \bmod 51$, it follows that

$$38^{-1} = 47$$

in $\mathbb{Z}_{51}$.