

Arithmetic Mod 11

Math for America · One-Time Pads and Secret Sharing

Name: _____

Why 11? We now work with the numbers $0, 1, 2, \dots, 10$ and wrap around at 11, exactly as we wrapped at 26 for the alphabet. The difference is that 11 is *prime*. That buys us something 26 cannot: every nonzero number has a *multiplicative inverse*, a partner it multiplies with to give 1. So we can divide, and that is what secret sharing needs. (Mod 26, try to solve $2x \equiv 1$: there is no answer.)

The rule for everything: do the ordinary arithmetic, then take the remainder on division by 11. $7 \times 8 = 56 = 5 \times 11 + 1$, so $7 \times 8 \equiv 1 \pmod{11}$. Negative numbers wrap up: $3 - 8 = -5 \equiv 6$, since $-5 + 11 = 6$.

Part 1 — Addition and subtraction.

$$\begin{array}{lll} 7 + 8 \equiv _____ & 9 + 9 \equiv _____ & 4 + 10 \equiv _____ \\ 6 + 5 \equiv _____ & 10 + 10 \equiv _____ & 3 + 9 \equiv _____ \\ 3 - 8 \equiv _____ & 0 - 1 \equiv _____ & 5 - 10 \equiv _____ \\ 2 - 9 \equiv _____ & 1 - 7 \equiv _____ & 4 - 4 \equiv _____ \end{array}$$

Part 2 — Multiplication. Multiply, then reduce.

$$\begin{array}{lll} 3 \times 4 \equiv _____ & 7 \times 8 \equiv _____ & 9 \times 9 \equiv _____ \\ 6 \times 10 \equiv _____ & 5 \times 7 \equiv _____ & 10 \times 10 \equiv _____ \\ 8 \times 4 \equiv _____ & 2 \times 6 \equiv _____ & 9 \times 7 \equiv _____ \end{array}$$

Part 3 — Inverses. For each a , find the number a^{-1} with $a \times a^{-1} \equiv 1 \pmod{11}$. Two of them you already found in Part 2. Is anything its own inverse?

a	1	2	3	4	5	6	7	8	9	10
a^{-1}	1									

Part 4 — Powers. Fill in each row by repeatedly multiplying by the base and reducing. Never let a number get bigger than 100: reduce after every step.

k	1	2	3	4	5	6	7	8	9	10
2^k	2	4	8							
3^k	3									
10^k	10									

- What is a^{10} for every base a in the table? (Fermat's little theorem: $a^{p-1} \equiv 1 \pmod{p}$.)
- Which base visits *every* nonzero number before returning to 1? Such a base is called a *generator*. How many steps does 3 take to return to 1? _____
- Compute, reducing as you go:

$$7^3 \equiv _____ \quad 5^4 \equiv _____ \quad 6^5 \equiv _____ \quad 4^7 \equiv _____ \quad 9^{10} \equiv _____ \quad 10^9 \equiv _____$$

Polynomials Mod 11

Math for America · One-Time Pads and Secret Sharing

Name: _____

Evaluating a polynomial. To find $f(x) \bmod 11$, compute each term separately and reduce it, then add the reduced terms and reduce once more. The reference page has a table of powers $x^k \bmod 11$, so you never have to compute $6^4 = 1296$ by hand. **Worked example:** $f(x) = 5 + 3x + 4x^2$ at $x = 6$. Mod 11, $6^2 = 36 \equiv 3$, so $4x^2 = 4 \times 3 = 12 \equiv 1$, and $3x = 18 \equiv 7$. Then $f(6) \equiv 5 + 7 + 1 = 13 \equiv 2$.

Part 5 — A quadratic. $f(x) = 4 + 7x + 3x^2$. One column per term, reduce each, then add.

x	x^2	$3x^2$	$7x$	4	$f(x)$
1				4	
2				4	
3				4	
4				4	

Part 6 — Degree 4. $f(x) = 7 + 2x + 9x^2 + 4x^3 + x^4$. First fill the powers, then the terms.

x	x^2	x^3	x^4	x^4	$4x^3$	$9x^2$	$2x$	7	$f(x)$
1								7	
2								7	
3								7	
4								7	
5								7	
6								7	

Part 7 — Degree 5. $f(x) = 6 + 10x + 3x^2 + 8x^3 + 2x^4 + 5x^5$. Same method, at $x = 1, \dots, 6$. The constant 6 is added at the end (no room for its column).

x	x^2	x^3	x^4	x^5	$5x^5$	$2x^4$	$8x^3$	$3x^2$	$10x$	$f(x)$
1										
2										
3										
4										
5										
6										

Why we care. In Shamir's scheme the *secret* is the constant term $f(0)$, and *share* i is the point $(i, f(i))$. You just made six shares of the secret 7 (Part 6) and six of the secret 6 (Part 7). A degree- d polynomial is pinned down by any $d + 1$ of its points and by no fewer, so Part 6 is a 5-of-6 scheme and Part 7 is 6-of-6. Look at your share values: do they leak anything about the secret?

Recovering the Secret

Math for America · One-Time Pads and Secret Sharing

Name: _____

2-of- N with a line. Choose a random slope a_1 and set $f(x) = s + a_1x$, where s is the secret. Share i is $f(i)$. Any two shares determine the line, so they determine $f(0) = s$; one share alone tells you nothing, because every slope is equally likely.

Recovering from two shares. Given (x_1, y_1) and (x_2, y_2) :

$$a_1 = (y_2 - y_1)(x_2 - x_1)^{-1}, \quad s = y_1 - a_1x_1 \pmod{11}.$$

The inverse comes from your Part 3 table. That is the only place division shows up.

Part 8. Two shares of a secret are $(2, 5)$ and $(7, 3)$.

1. $x_2 - x_1 \equiv$ _____, and its inverse is _____.
2. $y_2 - y_1 \equiv$ _____, so the slope is $a_1 \equiv$ _____.
3. The secret is $s = y_1 - a_1x_1 \equiv$ _____. Check by plugging both shares into $f(x) = s + a_1x$.
4. A third share is $(4, f(4))$. What is it? _____ Now recover s again from shares $(4, f(4))$ and $(7, 3)$ instead. Same answer?

T -of- N in general. A polynomial of degree $T - 1$ needs T points. With T shares $(x_1, y_1), \dots, (x_T, y_T)$ the secret is

$$s = f(0) = \sum_{i=1}^T y_i \prod_{j \neq i} \frac{x_j}{x_j - x_i} \pmod{11},$$

where each fraction means “multiply by the inverse.” This is Lagrange interpolation; for $T = 2$ it is exactly the line formula above.

Part 9 (challenge). Three shares of a secret from a *quadratic*: $(1, 3)$, $(2, 6)$, $(3, 0)$. Use the formula with $T = 3$.

i	y_i	$\prod_{j \neq i} \frac{x_j}{x_j - x_i}$ (write it out, then reduce)	$y_i \times$ product
1	3	$\frac{2}{2-1} \cdot \frac{3}{3-1} =$	
2	6	$\frac{1}{1-2} \cdot \frac{3}{3-2} =$	
3	0		

Secret $s \equiv$ _____. Then the hard question: with only *two* of these three shares, name three different secrets that would be consistent with them. (There are eleven.)

Reference: Tables Mod 11

A paper calculator. Row, then column.

Multiplication

$\times$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

Inverses

a	1	2	3	4	5	6	7	8	9	10
a^{-1}	1	6	4	3	9	2	8	7	5	10

Powers a^k (row a , column k)

$a \backslash k$	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1	3	9	5	4	1
4	4	5	9	3	1	4	5	9	3	1
5	5	3	4	9	1	5	3	4	9	1
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1	9	4	3	5	1
10	10	1	10	1	10	1	10	1	10	1

Addition

+	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	0
2	2	3	4	5	6	7	8	9	10	0	1
3	3	4	5	6	7	8	9	10	0	1	2
4	4	5	6	7	8	9	10	0	1	2	3
5	5	6	7	8	9	10	0	1	2	3	4
6	6	7	8	9	10	0	1	2	3	4	5
7	7	8	9	10	0	1	2	3	4	5	6
8	8	9	10	0	1	2	3	4	5	6	7
9	9	10	0	1	2	3	4	5	6	7	8
10	10	0	1	2	3	4	5	6	7	8	9

Answer Key

Part 1. $7 + 8 \equiv 4$, $9 + 9 \equiv 7$, $4 + 10 \equiv 3$, $6 + 5 \equiv 0$, $10 + 10 \equiv 9$, $3 + 9 \equiv 1$; $3 - 8 \equiv 6$, $0 - 1 \equiv 10$, $5 - 10 \equiv 6$, $2 - 9 \equiv 4$, $1 - 7 \equiv 5$, $4 - 4 \equiv 0$.

Part 2. $3 \times 4 \equiv 1$, $7 \times 8 \equiv 1$, $9 \times 9 \equiv 4$, $6 \times 10 \equiv 5$, $5 \times 7 \equiv 2$, $10 \times 10 \equiv 1$, $8 \times 4 \equiv 10$, $2 \times 6 \equiv 1$, $9 \times 7 \equiv 8$.

Part 3. Inverses of $1, \dots, 10$: $1, 6, 4, 3, 9, 2, 8, 7, 5, 10$. Only 1 and $10 \equiv -1$ are their own inverses.

Part 4. 2^k : $2, 4, 8, 5, 10, 9, 7, 3, 6, 1$. 3^k : $3, 9, 5, 4, 1, 3, 9, 5, 4, 1$. 10^k : $10, 1, 10, 1, 10, 1, 10, 1, 10, 1$. (1) $a^{10} \equiv 1$ in every row. (2) 2 is a generator; 3 returns to 1 after 5 steps, and 5 divides 10 . (3) $7^3 \equiv 2$, $5^4 \equiv 9$, $6^5 \equiv 10$, $4^7 \equiv 5$, $9^{10} \equiv 1$, $10^9 \equiv 10$.

Part 5. $f(1), \dots, f(4) = 3, 8, 8, 3$. **Part 6.** $f(1), \dots, f(6) = 1, 7, 8, 0, 3, 6$. **Part 7.** $f(1), \dots, f(6) = 1, 8, 6, 1, 10, 1$. The shares look like random numbers from 0 to 10 and carry no visible trace of the secret.

Part 8. $x_2 - x_1 = 5$, inverse 9 ; $y_2 - y_1 = -2 \equiv 9$, slope $a_1 = 9 \times 9 = 81 \equiv 4$; $s = 5 - 4 \times 2 = -3 \equiv 8$. So $f(x) = 8 + 4x$; check $f(2) = 16 \equiv 5$, $f(7) = 36 \equiv 3$. Third share: $(4, f(4)) = (4, 24 \equiv 2)$. From $(4, 2)$ and $(7, 3)$: $x_2 - x_1 = 3$, inverse 4 ; $y_2 - y_1 = 1$, slope $1 \times 4 = 4$; $s = 2 - 4 \times 4 = -14 \equiv 8$. Same secret.

Part 9. Row 1: $\frac{2}{1} \cdot \frac{3}{2} = 3$, times $y_1 = 3$ gives 9 . Row 2: $\frac{1}{-1} \cdot \frac{3}{1} = -3 \equiv 8$, times 6 gives $48 \equiv 4$. Row 3: $y_3 = 0$, so it contributes 0 whatever the product is. Secret $s = 9 + 4 = 13 \equiv 2$. (The polynomial is $f(x) = 2 + x^2$: $f(1) = 3$, $f(2) = 6$, $f(3) = 11 \equiv 0$.) With only two shares, every value of s from 0 to 10 fits some quadratic through them: pick any s , and the three points $(0, s)$, (x_1, y_1) , (x_2, y_2) determine one. That is why two shares reveal nothing.