

Cyclic Groups Mod 13

Math for America · Diffie–Hellman Key Exchange

Name: _____

The setting. Take the nonzero numbers mod 13: $\{1, 2, \dots, 12\}$. Multiply two of them and reduce, and you get another one; every element has an inverse. Twelve elements, one operation: a *group*. Today we care about one thing: what happens when you keep multiplying by the same number.

Order and generators. The *order* of a is the smallest $k \geq 1$ with $a^k \equiv 1 \pmod{13}$. The powers $a, a^2, a^3, \dots$ cycle with that period. If the order of a is 12, the powers of a visit *every* nonzero number; then a is a *generator* and the group is *cyclic*.

Part 1 — Warm-up. Multiply and reduce mod 13.

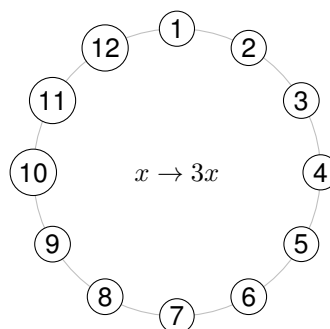
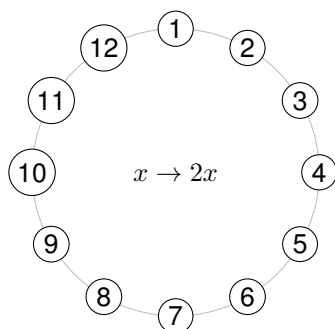
$$7 \times 9 \equiv \underline{\hspace{1cm}} \quad 11 \times 11 \equiv \underline{\hspace{1cm}} \quad 5 \times 8 \equiv \underline{\hspace{1cm}}$$

$$12 \times 12 \equiv \underline{\hspace{1cm}} \quad 6 \times 9 \equiv \underline{\hspace{1cm}} \quad 4 \times 10 \equiv \underline{\hspace{1cm}}$$

Part 2 — Powers. Fill each row, reducing after every multiplication. Then write the order of the base.

k	1	2	3	4	5	6	7	8	9	10	11	12	order
2^k	2	4	8										
3^k	3												
4^k	4												
5^k	5												
12^k	12												

- Which of the bases above is a generator? _____ What do all the orders you found have in common with 12?
- Once you have one generator g , the others are g^k for every k that shares no factor with 12. Use your row for 2^k to list all four generators mod 13: _____
- Multiplying by a shuffles the twelve numbers. On the left circle draw an arrow from each x to $2x \bmod 13$; on the right, from each x to $3x \bmod 13$. How many loops does each picture have, and how long are they?



Discrete Logarithms

Math for America · Diffie–Hellman Key Exchange

Name: _____

Running the cycle backwards. Since 2 is a generator, every nonzero $y \bmod 13$ is 2^k for exactly one k between 1 and 12. That k is the *discrete logarithm* of y (base 2): $\log_2 y = k$. Powers go forward; logs go backward.

Part 4 — The log table. Invert your 2^k row: for each y , find the k with $2^k \equiv y$.

y	1	2	3	4	5	6	7	8	9	10	11	12
$\log_2 y$		1										

Part 5 — Logs turn multiplication into addition. Because $2^i \times 2^j = 2^{i+j}$, and $2^{12} = 1$,

$$\log_2(xy) \equiv \log_2 x + \log_2 y \pmod{12}, \quad \log_2(x^n) \equiv n \cdot \log_2 x \pmod{12}.$$

Notice the modulus changed: logs live $\bmod 12 = 13 - 1$, not $\bmod 13$.

- 7×11 : $\log_2 7 = \underline{\hspace{1cm}}$, $\log_2 11 = \underline{\hspace{1cm}}$, sum $\bmod 12 = \underline{\hspace{1cm}}$, so $7 \times 11 \equiv 2^{\square} = \underline{\hspace{1cm}}$. Check by multiplying directly: $\underline{\hspace{1cm}}$
- 5^7 : $\log_2 5 = \underline{\hspace{1cm}}$, $7 \times \log_2 5 \bmod 12 = \underline{\hspace{1cm}}$, so $5^7 \equiv \underline{\hspace{1cm}}$. Check by computing $5^2, 5^4, 5^7$ directly: $\underline{\hspace{1cm}}$
- Big exponents are no harder: $2^{100} = 2^{100 \bmod 12} = 2^4 \equiv 3$.
Now compute $2^{1000} \equiv \underline{\hspace{1cm}}$ and $7^{50} \equiv \underline{\hspace{1cm}}$.

Part 6 — Why this matters. For $p = 13$ you built the complete log table in a minute. Now imagine p has 600 digits.

- Computing $g^k \bmod p$ for a 600-digit k takes about $2 \log_2 k \approx 4000$ multiplications by repeated squaring, a few milliseconds on a laptop. Explain why: how do you get g^8 from g^4 ? how do you get g^{13} from g^8, g^4, g^1 ?
- How many rows would the log table have? Compare with the *Powers of 2 and 10* ladder from the first session.
- The best known algorithms for discrete logs do beat “build the table,” but still take time that grows exponentially in the number of digits of p . This gap, **easy forward, hard backward**, is the whole basis of the next page.

Toy Diffie–Hellman

Math for America · Diffie–Hellman Key Exchange

Name: _____

The protocol. Everyone agrees in public on a prime p and a generator g . Here $p = 13$, $g = 2$.

	Alice	Bob
1. Pick a secret	a , any number from 1 to 11	b , any number from 1 to 11
2. Compute and <i>publish</i>	$A = g^a \bmod p$	$B = g^b \bmod p$
3. Receive the other's value	gets B	gets A
4. Compute the shared key	$K = B^a \bmod p$	$K = A^b \bmod p$

Both get the same K because $B^a = (g^b)^a = g^{ab} = (g^a)^b = A^b$. Eve sees p, g, A, B but not a or b .

Part 7 — Do it with a partner. Each of you picks a secret. Do *not* show it. Exchange only the public values.

	You	Your partner
Secret exponent (keep hidden)		
Public value = $2^{\text{secret}} \bmod 13$		
Partner's public value (received)		
Shared key = $(\text{received})^{\text{secret}} \bmod 13$		

Compare keys. If they differ, one of you slipped: find it. Then repeat with a new partner.

Part 8 — A worked round. Alice picks $a = 5$, Bob picks $b = 8$.

- $A = 2^5 \equiv \underline{\hspace{2cm}}$ $B = 2^8 \equiv \underline{\hspace{2cm}}$
- Alice computes $K = B^5$. Do it by repeated squaring: $B^2 \equiv \underline{\hspace{2cm}}$, $B^4 \equiv \underline{\hspace{2cm}}$, $B^5 = B^4 \cdot B \equiv \underline{\hspace{2cm}}$.
- Bob computes $K = A^8$: $A^2 \equiv \underline{\hspace{2cm}}$, $A^4 \equiv \underline{\hspace{2cm}}$, $A^8 \equiv \underline{\hspace{2cm}}$. Same key?
- Shortcut using logs: $K = g^{ab} = 2^{5 \cdot 8} = 2^{40 \bmod 12} = 2^{\square} \equiv \underline{\hspace{2cm}}$.

Part 9 — Eve. Eve sees $p = 13$, $g = 2$, A and B from Part 8. Using your log table from Part 4:

- $a = \log_2 A = \underline{\hspace{2cm}}$. Now Eve computes $K = B^a \equiv \underline{\hspace{2cm}}$. She needed only *one* of the two secrets.
- Mod 13 Eve wins instantly. In your own words, what has to be true about p for Alice and Bob to be safe?

Part 10 — A slightly bigger toy. $p = 23$, $g = 5$. The powers of 5 are on the reference page. Alice picks $a = 6$, Bob picks $b = 15$.

- From the table, $A = 5^6 \equiv \underline{\hspace{2cm}}$ and $B = 5^{15} \equiv \underline{\hspace{2cm}}$.
- Alice computes $K = B^6$ by repeated squaring (reduce mod 23 each time): $B^2 \equiv \underline{\hspace{2cm}}$, $B^4 \equiv \underline{\hspace{2cm}}$, $B^6 = B^4 \cdot B^2 \equiv \underline{\hspace{2cm}}$.
- Check with exponents: $K = 5^{6 \cdot 15} = 5^{90 \bmod 22} = 5^{\square} \equiv \underline{\hspace{2cm}}$. (Why mod 22 now?)

Reference: Tables Mod 13 and Mod 23

Powers $a^k \bmod 13$ (row a , column k), with the order of a

$a \backslash k$	1	2	3	4	5	6	7	8	9	10	11	12	order
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	3	6	12	11	9	5	10	7	1	12
3	3	9	1	3	9	1	3	9	1	3	9	1	3
4	4	3	12	9	10	1	4	3	12	9	10	1	6
5	5	12	8	1	5	12	8	1	5	12	8	1	4
6	6	10	8	9	2	12	7	3	5	4	11	1	12
7	7	10	5	9	11	12	6	3	8	4	2	1	12
8	8	12	5	1	8	12	5	1	8	12	5	1	4
9	9	3	1	9	3	1	9	3	1	9	3	1	3
10	10	9	12	3	4	1	10	9	12	3	4	1	6
11	11	4	5	3	7	12	2	9	8	10	6	1	12
12	12	1	12	1	12	1	12	1	12	1	12	1	2

Discrete logs base 2, mod 13

y	1	2	3	4	5	6	7	8	9	10	11	12
$\log_2 y$	12	1	4	2	9	5	11	3	8	10	7	6

Inverses mod 13

a	1	2	3	4	5	6	7	8	9	10	11	12
a^{-1}	1	7	9	10	8	11	2	5	3	4	6	12

Multiplication mod 13

$\times$	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	1	3	5	7	9	11
3	3	6	9	12	2	5	8	11	1	4	7	10
4	4	8	12	3	7	11	2	6	10	1	5	9
5	5	10	2	7	12	4	9	1	6	11	3	8
6	6	12	5	11	4	10	3	9	2	8	1	7
7	7	1	8	2	9	3	10	4	11	5	12	6
8	8	3	11	6	1	9	4	12	7	2	10	5
9	9	5	1	10	6	2	11	7	3	12	8	4
10	10	7	4	1	11	8	5	2	12	9	6	3
11	11	9	7	5	3	1	12	10	8	6	4	2
12	12	11	10	9	8	7	6	5	4	3	2	1

Powers of 5 mod 23 (5 is a generator; the cycle has length 22)

k	1	2	3	4	5	6	7	8	9	10	11
5^k	5	2	10	4	20	8	17	16	11	9	22
k	12	13	14	15	16	17	18	19	20	21	22
5^k	18	21	13	19	3	15	6	7	12	14	1

Answer Key

Part 1. $7 \times 9 \equiv 11, 11 \times 11 \equiv 4, 5 \times 8 \equiv 1, 12 \times 12 \equiv 1, 6 \times 9 \equiv 2, 4 \times 10 \equiv 1$.

Part 2. 2^k : 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1 (order 12). 3^k : 3, 9, 1, 3, 9, 1, 3, 9, 1, 3, 9, 1 (order 3). 4^k : 4, 3, 12, 9, 10, 1, 4, 3, 12, 9, 10, 1 (order 6). 5^k : 5, 12, 8, 1, 5, 12, 8, 1, 5, 12, 8, 1 (order 4). 12^k : 12, 1, 12, 1, 12, 1, 12, 1, 12, 1, 12, 1 (order 2).

Part 3. (1) Only 2 is a generator among these; every order divides 12 (Lagrange's theorem). (2) $k \in \{1, 5, 7, 11\}$ gives $2, 2^5 = 6, 2^7 = 11, 2^{11} = 7$: the generators are 2, 6, 7, 11. (3) $x \rightarrow 2x$: one loop of length 12 ($1 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 3 \rightarrow 6 \rightarrow 12 \rightarrow 11 \rightarrow 9 \rightarrow 5 \rightarrow 10 \rightarrow 7 \rightarrow 1$). $x \rightarrow 3x$: four loops of length 3: (1, 3, 9), (2, 6, 5), (4, 12, 10), (7, 8, 11). The loop length is the order of the multiplier.

Part 4. $\log_2 y$ for $y = 1, \dots, 12$: 12, 1, 4, 2, 9, 5, 11, 3, 8, 10, 7, 6.

Part 5. (1) $11 + 7 = 18 \equiv 6 \pmod{12}$, so $7 \times 11 \equiv 2^6 = 12$; directly $77 = 5 \cdot 13 + 12$. (2) $\log_2 5 = 9, 63 \equiv 3 \pmod{12}$, so $5^7 \equiv 2^3 = 8$; directly $5^2 \equiv 12, 5^4 \equiv 1, 5^7 = 5^4 \cdot 5^2 \cdot 5 \equiv 60 \equiv 8$. (3) $1000 \equiv 4 \pmod{12}$ so $2^{1000} \equiv 3; 7^{50}: \log_2 7 = 11, 550 \equiv 10 \pmod{12}, 2^{10} \equiv 10$ (or $7^{48} = 1, 7^2 = 49 \equiv 10$).

Part 6. (4) $g^8 = (g^4)^2; g^{13} = g^8 \cdot g^4 \cdot g^1$ since $13 = 8 + 4 + 1$ in binary. Each squaring doubles the exponent, so 600 digits (≈ 2000 bits) needs about 2000 squarings and at most 2000 extra multiplications. (5) About 10^{600} rows; the ladder tops out at 10^{80} atoms in the universe.

Part 8. $A = 6, B = 9$. Alice: $9^2 = 81 \equiv 3, 9^4 \equiv 9, 9^5 = 9 \cdot 9 = 81 \equiv 3$. Bob: $6^2 = 36 \equiv 10, 6^4 \equiv 100 \equiv 9, 6^8 \equiv 81 \equiv 3. K = 3$. Shortcut: $40 \equiv 4 \pmod{12}, 2^4 = 3$.

Part 9. $a = \log_2 6 = 5; K = 9^5 \equiv 3$. Safety needs p so large that no table and no cleverer algorithm can find a from $A = g^a$: in practice p of 2048 bits or more.

Part 10. $A = 8, B = 19$. $19^2 = 361 \equiv 16, 19^4 \equiv 256 \equiv 3, 19^6 \equiv 3 \cdot 16 = 48 \equiv 2$. Exponents: $90 \equiv 2 \pmod{22}, 5^2 = 25 \equiv 2$. Mod 22 because the powers of 5 repeat with period $22 = 23 - 1$.