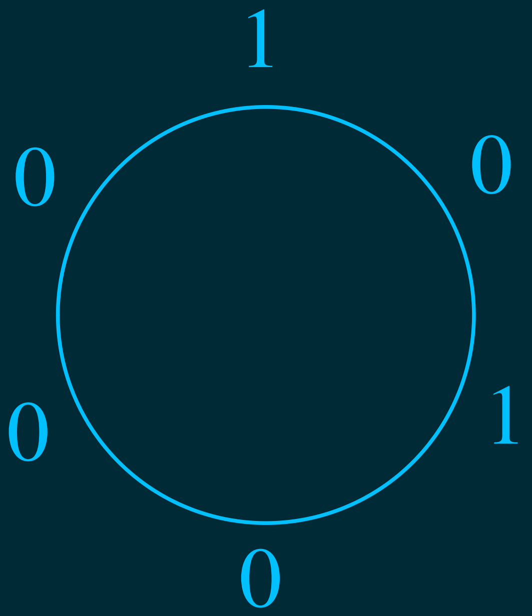
You have six integers $a_1, a_2, a_3, a_4, a_5, a_6$ arranged in the clockwise fashion on a circle. Their initial values are $1, 0, 1, 0, 0, 0$, respectively. You then run a loop, each iteration of which takes two consecutive integers (that is, (a_1, a_2) or (a_2, a_3) or $\cdots$ or (a_6, a_1)), and increments both the chosen integers by 1. Your goal is to make all the six integers equal. Propose a way to achieve this using the above loop (that is, specify which pairs you choose in different iterations), or prove that this cannot be done.



$S = a_1 - a_2 + a_3 - a_4 + a_5 - a_6$

Initial value $= 2$

Each iteration keeps this value.

Target $= 0$ is not achievable

What does the following function return upon the input of two positive integers a, b? Prove it.

```
int f ( int a, int b )
{
    int x, y, u, v;

    x = u = a; y = v = b;
    while (x != y) {
        if (x > y) {
            x = x - y;
            u = u + v;
        } else {
            y = y - x;
            v = u + v;
        }
    }
    return (u + v)/2;
}
```

$v(x-y) + (u+v)y$

$= vx - vy + uy + vy$

$= vx + uy = 2ab$

$x = y = \gcd(a, b)$

$(v+u)\gcd(a, b) = 2ab$

$\frac{u+v}{2} = \frac{ab}{\gcd(a,b)} = \mathrm{lcm}(a,b)$

- $\gcd(x, y) = \gcd(a, b)$
- $vx + uy = 2ab$

Let A be a sorted array of $n \geqslant 2$ integers with repetitions allowed. Consider the following variant of binary search for x in A. Prove by an invariance property of the loop that the function returns the index of the *first* occurrence of x in A (or -1 if x is not present in A).

(last)

```
int first ( int A[], int n, int x )
{
   int L, R, M;

   if ( (A[0] > x) || (A[n-1] < x) ) return -1;
   if (A[0] == x) return 0;
   L = 0; R = n-1;
   while (R - L > 1) {
      M = (L + R + 1) / 2;
      if (A[M] >= x) R = M; else L = M;
   }
   if (A[R] == x) return R;
   else return -1;
}
```

$$A[L] < x \leq A[R]$$

Let a, b be two positive integers, and $d = \gcd(a,b) = ua + vb$ with $u, v \in \mathbb{Z}$. Prove that u and v can be so chosen that $|u| < \dfrac{b}{d}$ and $|v| < \dfrac{a}{d}$.

$$1 = u(a/d) + v(b/d) \qquad u = q\frac{b}{d} + r$$

$$= \left(u - q\frac{b}{d}\right)\frac{a}{d} + \left(v + q\frac{a}{d}\right)\frac{b}{d} \qquad 0 \leq r < \frac{b}{d}$$

$$= r\frac{a}{d} + s\frac{b}{d} \qquad \left(r < \frac{b}{d}\right)$$

$$|s| = \left|\frac{1 - r\frac{a}{d}}{b/d}\right| = \frac{r\frac{a}{d} - 1}{b/d} < \frac{r\frac{a}{d}}{b/d} < \frac{a}{d}$$

$$(r \neq 0)$$

Let a, b, c be non-zero integers. Prove that the equation

$$ax + by = c$$

has solutions in integer values of x and y if and only if

$$\gcd(a, b) \mid c.$$

$d = \gcd(a, b)$

$\Rightarrow$ $ax + by = c$ for some $x, y \in \mathbb{Z}$

$d \mid a$, $d \mid b$ $\Rightarrow$ $d \mid ax + by$ $\Rightarrow$ $d \mid c$

$\Leftarrow$ $c = kd = k(ua + vb)$

$= \underbrace{(ku)}_{x} a + \underbrace{(kv)}_{y} b$

Prove that if $2^n - 1$ is prime, then n is prime.

n is composite.

$n = ab \qquad 1 < a, b < n$

GIMPS

$(2^a - 1) \mid (2^n - 1)$

$\rightarrow$ proper divisor

Lucas-Lehmer test

(Marine) Mersenne primes

Suppose that $2^n - 1$ is prime. Prove that

$$2^{n-1}(\underline{2^n - 1}) \quad p$$

is a perfect number.

$$6 = 1 + 2 + 3$$

$$28 = 1 + 2 + 4 + 7 + 14$$

$$496$$

$$1, 2, 4, \ldots, 2^{n-1}$$

$$p, 2p, 4p, \ldots, 2^{n-2} p$$

Add them.

Every even perfect numbers must be of this form.

You pick nine distinct points with integer coordinates in the three-dimensional space. Prove that there must exist two of these nine points—call them P and Q—such that the line segment PQ has a point (other than P and Q) on it with integer coordinates.

(odd/even, odd/even, odd/even)

8 possibilities

P, Q with the same parities

Consider $\frac{P+Q}{2}$

Let $n \geqslant 10$ be an integer. You choose n distinct elements from the set $\{1, 2, 3, \ldots, n^2\}$. Prove that there must exist two disjoint non-empty subsets of the chosen numbers, whose sums are equal.

subset sum $< n^3$

\# of subsets (non-empty) $= 2^n - 1$

$2^n - 1 > n^3$

$\sum_{a \in A} a = \sum_{b \in B} b$.

$A \neq B$

what if $A \cap B \neq \emptyset$?

$A' = A \setminus A \cap B$

$B' = B \setminus A \cap B$

Let ξ be an irrational number. Prove that given any real $\varepsilon > 0$ (no matter how small), there exist integers a, b such that $0 < a\xi - b < \varepsilon$.

Choose an integer $n > 1/\epsilon$.

$[\ )[\ )[\ )\ \cdots\ [\ )$

$0 \quad \frac{1}{n} \quad \frac{2}{n} \quad \frac{3}{n} \quad \cdots \quad \frac{n-1}{n} \quad 1$

$\{x\}$ = fractional part of x.

$\{\xi\}, \{2\xi\}, \{3\xi\}, \ldots, \{(n+1)\xi\}$

$i \neq j$ $\quad \{i\xi\}, \{j\xi\}$ go to the same subinterval

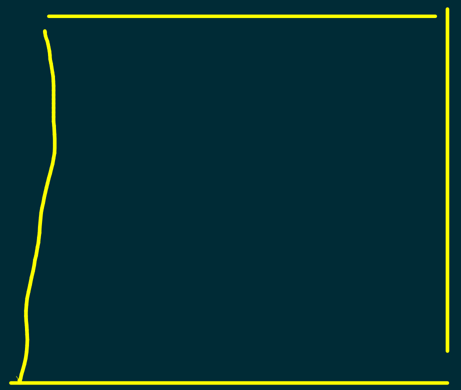
$\{\pi\} = 0.14159265\ldots$

$$0 < \{i\xi\} - \{j\xi\} < 1/n$$

$$\{i\xi\} = i\xi - u \qquad \{j\xi\} = j\xi - v$$

$$\underbrace{(i-j)}_{a}\xi - \underbrace{(v-u)}_{b} < \frac{1}{n} < \epsilon$$

$36 < 40$



A spread does not increase the no of inf / non-inf boundary edges.