最大公約数を求める: Euclid の互除法

用語:
約数: 「a は b の約数である」（a も b も自然数として）
b を a で割り算すると割り切れる。もしくは 適当な自然数 c が存在し b = a × c と表せる
例: 6 の約数: 1, 2, 3, 6
C で書くと、 b % a == 0 が成り立つ

倍数:「bは a の倍数である」（a も b も自然数として）
b を a で割り算すると割り切れる、もしくは 適当な自然数 c が存在し、b = a × c と表せる
例: 2 の倍数: 2, 4, 6, 8, …
「a が b の約数ならば、必ず b は a の倍数であり、逆も成り立つ」（a も b も自然数とする）

公約数:「a は b と c の公約数である」（a, b, c は自然数として）
a は b の約数であり、かつ a は c の約数でもある (a は b と c の共通の約数）
例: 12 と 18 の公約数: 1, 2, 3, 6
次を満たす適当な自然数 u, v が存在: b = u×a かつ c = v×a

公倍数:「x は b と c の公倍数である」（x, b, c は自然数として）
b は x の約数であり、かつ c も x の約数でもある。
例: 12 と 18 の公約数: 1, 2, 3, 6
次を満たす適当な自然数 u, v が存在: x = u×b かつ x = v×c

互いに素:「u と v は互いに素である」(u も v も自然数として）
u と v の公約数はただひとつしかない（1だけ）
(u と v は素数でなくてもこれは成り立つ。例えば 4 と 9)

最大公約数:「a は b と c の最大公約数である」（a, b, c は自然数として）
⇔ a は b と c の公約数であり、そのうちの最大のもの(ただひとつ存在）
次を満たす適当な自然数 u, v が存在: b = u×a かつ c = v×a かつ u と v は互いに素
例: 12 と 18 の最大公約数は 6

最小公倍数:「x は b と c の最小公倍数である」（x, b, c は自然数として）
⇔ x は b と c の公倍数であり、そのうちの最小のもの(ただひとつ存在）
次を満たす適当な自然数 u, v が存在: x = u×b かつ x = v×c かつ u と v は互いに素
例: 12 と 18 の最小公倍数は 36

Euclid の互除法:
b と c の最大公約数を求める。(b ≧ c と仮定)
ここで最大公約数を a とおくと、
次を満たす適当な自然数 u, v が存在: b = u×a かつ c = v×a かつ u と v は互いに素
しかも、 u ≧ v ≧ 1
★ r = b % c (bを c で割ったあまり) とする
すると r = (u % v) ×a と表される。(u ≧ v ≧ u % v ≧ 0)
r == 0 ならば u%v==0 を意味する。これは、「u と v が互いに素」から v=1 を意味。
つまり、(この時） c = a となる。したがって c の値を返して終了
そうでなければ(r != 0 ならば)
b = c , c = r として、★に行く
これは、u ,v = v, u % v とすると、b = u×a、c = v×a と表されることを意味
（しかもこのとき u と v は互いに素であることは保証される）

2 個の整数を引数とし、その最大公約数を返す関数 gcd:

```
int gcd(int b, int c) {
        int r;
        if (b < c) {
            r = b ; b = c;  c = r;
        }
        r = b % c;
         if (r == 0) {
                return c;
        }
        return gcd(c, r);          //  次は b← c ;  c ← r となる
}
```

2 個の整数を引数とし、その最小公倍数を返す関数 lcm:

```
int  lcm(int b, int c) {
        int a = gcd(b,c) ;   // a を最大公約数とする
         // b = u×a、   c = v× a と表される
        // 求めるのは、x = u ×v×a
        return  (b / a) * c;
}
```

3 個の整数を引数とし、その最大公約数を返す関数 gcd3

引数を x, y, z とし、a を求める最大公約数とすると
適当な整数 u, v, w があり、x = u×a, y = v×a、z = w×a と表される
(u, v, w の最大公約数は 1)
ここで u と v の最大公約数を α (α は自然数)と書くと　gcd(x,y)=α×a と表される。
これと z (=w×a) との最大公約数を求めると、(つまり、gcd(α×a, w×a)) a が得られる
注: もしも α と w の最大公約数が「1 でない数」とすると、「a が x,y,z の最大公約数」という仮定に反することになる
よって、　gcd3(x,y,z) は gcd(gcd(x,y), z)　で得られる。

3個の整数を引数とし、その最小公倍数を返す関数 lcm3:

引数を a, b, c とし、x を求める最小公倍数とする
適当な自然数 p, q, r, s,t,u,v を用いて a = r×p×q×s, b = r×p×t×u, c = r×q×t×v　と表せる
すると求める最小公倍数は x = r×p×q×t×s×u×v と表される
(rは a,b,c の最大公約数、p は a/r と b/r の最大公約数、t は b/r と c/r の最大公約数、
q は a/r と c/r の最大公約数, s は a/(r×p×q), u は b/(r×p×t), v は c/(r×q×t))
以上から、　lcm(x,y)= (r×p×q)×s×t×u　と表される。これは c と r×q×t という最大公約数を持つ
よって、lcm(lcm(x,y), z) = (r×p×q×t)×s×u×v となり、これは求める最小公倍数に等しい
以上から、lcm3(x,y,z) = lcm(lcm(x,y), z)