270 (greatest common divisor) Write a program to find the greatest common divisor of

(a) two positive integers.

(b) two integers (not necessarily positive ones) that are not both zero.

(c) three positive integers. One method is to find the greatest common divisor of two of them, and then find the greatest common divisor of that and the remaining number, but there is a better way.

After trying the question, scroll down to the solution.

(a) two positive integers.

§ Let $gcd\ a\ b$ be the greatest common divisor of a and b, defined as

$$a, b: (nat+1) \times gcd\ a\ b \ \land\ \forall d: (a, b: (nat+1) \times d)\cdot\ d \le gcd\ a\ b$$

Then

$$a>b \ \Rightarrow\ gcd\ a\ b \ = \ gcd\ (a-b)\ b$$

$$a<b \ \Rightarrow\ gcd\ a\ b \ = \ gcd\ a\ (b-a)$$

$$gcd\ a\ a \ = \ a$$

Let all variables (except time) be of type positive natural. A program for gcd is

```
$a' = b' = gcd\ a\ b \ \land\ t' \le t + a{\uparrow}b \ \Longleftarrow$
    if $a>b$ then $a:= a-b$.  $t:= t+1$.  $a' = b' = gcd\ a\ b \ \land\ t' \le t + a{\uparrow}b$
    else if $a<b$ then $b:= b-a$.  $t:= t+1$.  $a' = b' = gcd\ a\ b \ \land\ t' \le t + a{\uparrow}b$
        else $ok$ fi fi
```

Here are more properties of gcd.

$$gcd\ (2{\times}a)\ (2{\times}b) \ = \ 2 \times gcd\ a\ b$$

$$gcd\ (2{\times}a)\ (2{\times}b+1) \ = \ gcd\ a\ (2{\times}b+1)$$

$$gcd\ (2{\times}a+1)\ (2{\times}b) \ = \ gcd\ (2{\times}a+1)\ b$$

$$a>b \ \Rightarrow\ gcd\ (2{\times}a+1)\ (2{\times}b+1) \ = \ gcd\ (a-b)\ (2{\times}b+1)$$

$$a<b \ \Rightarrow\ gcd\ (2{\times}a+1)\ (2{\times}b+1) \ = \ gcd\ (2{\times}a+1)\ (b-a)$$

These properties allow us to write a gcd program that runs in $log\ (a{\uparrow}b)$ time.

```
$a' = b' = gcd\ a\ b \ \land\ t' \le t + log\ (a{\uparrow}b) \ \Longleftarrow$
    if $a=b$ then $ok$
    else if $even\ a$
        then if $even\ b$
            then $a:= a/2$.  $b:= b/2$.  $t:= t+1$.
                $a' = b' = gcd\ a\ b \ \land\ t' \le t + log\ (a{\uparrow}b)$.
                $a:= 2{\times}a$.  $b:= 2{\times}b$
            else $a:= a/2$.  $t:= t+1$.
                $a' = b' = gcd\ a\ b \ \land\ t' \le t + log\ (a{\uparrow}b)$ fi
        else if $even\ b$
            then $b:= b/2$.  $t:= t+1$.  $a' = b' = gcd\ a\ b \ \land\ t' \le t + log\ (a{\uparrow}b)$
            else if $a>b$
                then $a:= (a-b)/2$.  $t:= t+1$.
                    $a' = b' = gcd\ a\ b \ \land\ t' \le t + log\ (a{\uparrow}b)$
                else $b:= (b-a)/2$.  $t:= t+1$.
                    $a' = b' = gcd\ a\ b \ \land\ t' \le t + log\ (a{\uparrow}b)$ fi fi fi fi
```

(b) two integers (not necessarily positive ones) that are not both zero.

(c) three positive integers. One method is to find the greatest common divisor of two of them, and then find the greatest common divisor of that and the remaining number, but there is a better way.