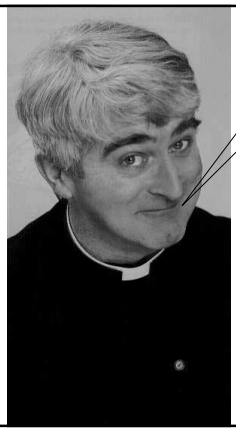
AF2



Primes, gcd, some examples, reading

Primes

- p>1 is ***prime*** if the only positive factors are 1 and p
- if p is not prime it is ***composite***

The Fundamental Theorem of Arithmetic

Every positive integer can be expressed as a unique product of primes

$$n = \prod_{i=1}^{k} p_i^{e_i}$$

How many prime numbers are there? Is there a largest prime number?

- assume we know all the prime numbers
  - let p be the largest prime
  - multiply all the primes together
  - add 1
  - call this n
- n is not divisible by 2, we get remainder 1
- n is not divisible by 3, we get remainder 1
- n is not divisible by 5, we get remainder 1
- …
- n is not divisible by p, we get remainder 1
- But, by the FTA we know n has a prime factorisation
- Therefore n must have a prime divisor > p
- Therefore there is no greatest prime

Due to Euclid

PRIMES

If n is composite n has a prime divisor $\leq \sqrt{n}$

$$\text{composite}(n) \rightarrow n = a.b$$

$$a \leq \sqrt{n} \vee b \leq \sqrt{n}$$

$$\neg(a > \sqrt{n} \wedge b > \sqrt{n})$$

Therefore, the divisor a or b is either prime or due to the fundamental theorem of arithmetic, can be expressed as a product of primes

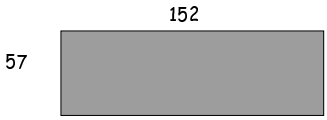
$$\therefore n \text{ has a divisor} \leq \sqrt{n}$$

How big a prime do we want?

for RSA encryption
"The most efficient factorisation methods (1999) require billions of years to factor 400 digit integers. Consequently … when 200 digit primes … messages encrypted … cannot be found in a reasonable time."

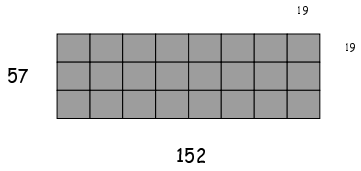
"When new factorisation techniques are found … it will be necessary to use larger primes to ensure secrecy/security of messages."

gcd, a geometric view

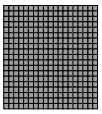


☺ We have a floor to tile
☺ The floor is 57 units wide and 152 units long
☺ What is the largest square tile we can use to tile the floor
☺ this will be the least number of square tiles!

gcd, a geometric view



☺ Find gcd(57,152)
☺ 19 is the answer
☺ we need 24 tiles



Theorem

- ☞ when a = b.q + r
- ☞ greatest common divisor of a and b

is also

- ☞ greatest common divisor of b and r
- ☞ i.e. gcd(a,b) = gcd(b,r)

A proof follows

The proof is based on what we already know about division

RTP: gcd(a,b) = gcd(b,r) where a = b.q + r

Sketch of the proof
Show that common divisors of a and b are also common divisors of b and r

(1) show that if some d|a and d|b then d|r
(2) show that if some d|b and d|r then d|a
(3) conclude that a common divisor of a and b is also a common divisor of b and r
(4) consequently gcd(a,b) = gcd(b,r)

RTP: gcd(a,b) = gcd(b,r) where a = b.q + r

(1) show that if some d|a and d|b then d|r

a = b.q + r
∴a - b.q = r

We have already proved that

- if d|b then d|b.q
- if d|a and d|b.q then d|(a - b.q)

since d|a and d|b.q it follows that d|(a - b.q)
since (a - b.q) = r it follows that d|r

Consequently a common divisor of a and b also divides r

RTP: gcd(a,b) = gcd(b,r) where a = b.q + r

(2) show that if some d|b and d|r then d|a

a = b.q + r

We have already proved that

- if d|b then d|b.q
- if d|b.q and d|r then d|(b.q + r)

since d|b.q and d|r it follows that d|(b.q + r)
since (b.q + r) = a it follows that d|a

Consequently a common divisor of b and r also divides a

RTP: gcd(a,b) = gcd(b,r) where a = b.q + r

(3) conclude that a common divisor of a and b is also a common divisor of b and r

From (1) and (2) we have proved that

- ☆ a common divisor of a and b is also a divisor of r
- ☆ a common divisor of b and r is also a divisor of a
- ☆ consequently a common divisor of a and b is also a common divisor of b and r

RTP: gcd(a,b) = gcd(b,r) where a = b.q + r

(4) consequently gcd(a,b) = gcd(b,r)

From (3) we can conclude that the greatest common divisor of a and b is also a greatest common divisor of b and r

This suggests an algorithm

- given a and b
- if a = 0 then b is the gcd
- if b = 0 then a is the gcd
- otherwise
  - a ÷ b = q remainder r
  - we have established that we can substitute
  - gcd(a,b) with gcd(b,r)
  - now compute gcd(b,r)
    - note, r is decreasing!

gcd

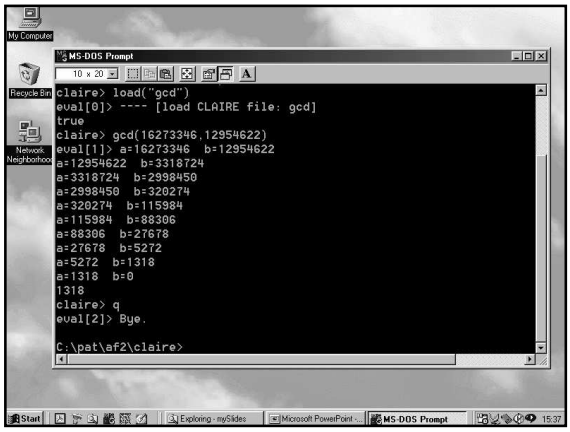
- We have shown that when a = b.q + r
  - any divisor of a and b is also a divisor of b and r
  - consequently gcd(a,b) = gcd(b,r)
- We state that gcd(0,b) = b and gcd(a,0) = a
  - therefore, there is nothing to do if a or b is zero
- Due to our theorem
  - we can reduce gcd(a,b) to a simpler problem gcd(b,r)
  - at each iteration we replace
    - b with r where $0 \leq r < b$
    - at each iteration b decreases
    - eventually this must terminate with b = 0
    - and as we said, we are then done
      - and a is the answer!

gcd(a,b)

- gcd(a,b)
  - if b = 0
  - then a
  - else gcd(b,a mod b)

- (0) gcd(a,b)
  - (1) if b = 0 goto 6
  - (2) let r := a mod b
  - (3) a := b
  - (4) b := r
  - (5) goto (1)
  - (6) return(a)

```
gcd(a,b)
    while b ≠ 0
    do begin
        r := a mod b;
        a := b;
        b := r;
       end;
    a
```



[gcd(a:integer,b:integer) : integer
 -> if (b = 0) a else gcd(b,a mod b)]

[relativePrime(a:integer,b:integer) : boolean
 -> gcd(a,b) = 1]

Try
- gcd(414,662) and then gcd(662,414)
- gcd(120,500) and gcd(500,120)
- list all numbers relative prime to 22

Numbers

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$$

- A number to the base b
  - it has k+1 terms
  - the a's are all in the range 0 to b-1

- what is
  - 10101101 base 2 in base 10
  - peter base 26 in base 10

Numbers

- Can you do arithmetic in different bases?
  - I expect so (see pages 169-177)
- Can you do addition, multiplication, subtraction, division
  - in different bases? (I expect so)
- Do you know the algorithm for this?
  - Again, I expect so.