

MEI Conference, 2010

Brush Up

On your Number Theory

Oscar Gregan

noel.gregan@virgin.net

While we are waiting!

Mental arithmetic and Algebraic aids.

Can we do the following without calculator, or pencil and paper?

$$39 \quad 41$$

$$68$$

$$45^2$$

$$46^2$$

$$44^2$$

$$93$$

RELATED ALGEBRA:

$$39 \quad 41 = \quad = 1599; \quad 68 \quad = 70^2 - 4 = 4896.$$

$$45^2 = 4$$

$$46^2 = 45^2 +$$

$$44^2 = 45^2 -$$

—

—

—

=

$$- = 380.25$$

$$93 \quad = 90$$

Find the prime factors of N - then what next?

Writing numbers as products of their prime factors is a common GCSE exam question. Follow-on problems are quite limited – finding LCMs and HCFs or perhaps finding square roots of large numbers which have integer roots.

How about these problems:

Using prime decomposition

- Find the square root of 17424
- How many factors has 2010?
- Find all the numbers less than 120 that have exactly 10 factors
- Find the smallest number that has exactly 18 factors.
- Find how many zeros there are after the last non-zero digit in 30!

Divisibility tests are useful for finding the prime factors of large numbers especially the tests for 3 and 11.

❖ Divisibility tests:

- At a glance we can tell if 2, 5 & 10 are factors of a bigger integer
- 4 & 8?
- 3 & 9?
- 11?
- 7??

Proof of these divisibility tests.

Test for 4:

Let $N = 100m + p$. $4|N \Leftrightarrow 4|100m + p$. So if 4 divides into the number formed by the last two digits of N then $4|N$.

Test for 8:

Let $N = 1000m + p$. $8|N \Leftrightarrow 8|1000m + p$. So if 8 divides into the number formed by the last three digits of N then $8|N$.

Test for 3:

Let $N = 1000a + 100b + 10c + d$. If $3|N$ then $N \pmod{3} = 0$. As $1000 \pmod{3} = 1$, $100 \pmod{3} = 1$, $10 \pmod{3} = 1$, $1 \pmod{3} = 1$. So if 3 divides into the sum of the digits, then $3|N$.

Test for 9:

Let $N = \dots 10c + d$. If $9 \mid N$ then $N \pmod{9} = 0$. As $10 \equiv 1 \pmod{9}$, $N \equiv \dots 10 \equiv 1 \pmod{9}$. So if 9 divides into the sum of the digits, then $9 \mid N$.

Test for 11:

Again let $N = \dots 10c + d$. If $11 \mid N$ then $N \pmod{11} = 0$.

As $10 \equiv -1 \pmod{11}$, $N \equiv \dots 10 \equiv -1 \pmod{11}$. So if we add 1st digit + 3rd digit + 5th digit + ... then add 2nd + 4th + 6th + ... and if 11 divides into the difference of the two sums then $11 \mid N$.

Test for 7:

This test is not widely used probably because it is often as quick to do the actual division. It is included here for interest.

Suppose N is divisible by 7. We can write $N \equiv 0 \pmod{7}$. [N is a positive integer]

Let $N = 10M + R$

$7 \mid N \Rightarrow 10M + R \equiv 0 \pmod{7}$.

$\times 5$: $50M + 5R \equiv 0 \pmod{7}$.

As $50 \equiv 1 \pmod{7}$ and $5 \equiv -2 \pmod{7}$

So $N = 10M + R \equiv M - 2R \equiv 0 \pmod{7}$

Example:

Does $7 \mid 8827$?

$8827 = 882 \times 10 + 7 \pmod{7} = 882 - 14 \pmod{7} = 868 \pmod{7} = 86 - 16 \pmod{7} = 70 \pmod{7}$

So $7 \mid 8827$.

This approach can be used for many primes.

A Test for Divisibility by 13:

Let $N = 10M + R$

$13 \mid N \Rightarrow 10M + R \equiv 0 \pmod{13}$.

$\times 4$: $40M + 4R \equiv 0 \pmod{13}$.

As $40 \equiv 1 \pmod{13}$. So $N = 10M + R \equiv M + 4R \equiv 0 \pmod{13}$

Example:

Does $13 \mid 8827$?

$8827 = 882 \times 10 + 7 \pmod{13} = 882 + 28 \pmod{13} = 910 \pmod{13} = 91 \pmod{13}$. So $13 \mid 8827$.

Exercise:

Devise a test for 23 and test whether the following numbers are divisible by 7 or 13 or 23.

- 1) 2898 2) 6864 3) 12992

Having written a number in terms of its prime factors, we can complete the tasks listed earlier. A key result is listed below:

$$\text{If } N = (p_1)^a (p_2)^b (p_3)^c \dots (p_r)^r$$

Then

| |
|---|
| Numbers of factors of $N = (a + 1)(b + 1)(c + 1) \dots (r + 1)$. |
|---|

where $p_1, p_2, p_3, \dots, p_r$ are the prime factors of N and a, b, c, \dots are integers ≥ 0

Example:

- (i) How many factors has 360?

$360 = 2^3 \times 3^2 \times 5$. So number of factors $= (3 + 1)(2 + 1)(1 + 1) = 4 \times 3 \times 2 = 24$ factors.

- (ii) Find all the numbers less than 120 that have exactly 10 factors.

$$(a + 1)(b + 1)(c + 1) \dots (r + 1) = 10 \text{ but } 10 = 2 \times 5$$

$$a + 1 = 5 \text{ and } b + 1 = 2 \Rightarrow a = 4 \text{ \& } b = 1 \quad (p_1)^4 (p_2)^1 \leq 120.$$

Possible solutions are $2^4 \times 3 = 48$; $2^4 \times 5 = 80$; $2^4 \times 7 = 112$

- (iii) Find the smallest number that has exactly 18 factors.

$$(a + 1)(b + 1)(c + 1) \dots (r + 1) = 18.$$

$$2 \times 3 \times 3 \Rightarrow a = 1, b = 2, c = 2. N = 2^2 \times 3^2 \times 5 = 180.$$

$$3 \times 6 = (a + 1)(b + 1) \Rightarrow a = 2, b = 5, \Rightarrow N = 2^3 \times 3^6 = 2916.$$

$2 \times 2 \times 9$ gives $N = 256$ and 1×18 gives $N = 2^{17}$ so 180 is our smallest number.

Decimal Fractions; Terminating and Recurring

In recent years questions involving terminating and recurring decimals have begun to appear on GCSE papers. Again these questions have had limited scope as the exam candidates have either been asked (a) to identify whether particular fractions are recurring or terminating or (b) to convert recurring decimals to fractions.

- Decimal fractions are terminating or recurring only.
- Terminating decimals occur when the denominator's prime factors are powers of 2 &/or 5 only as 2 and 5 are the only primes which divide into 10.
- Fermat's Little Theorem helps us understand the size of the recurring cycle:

We can only conclude from this that the cycle of the fraction, $1/p$, where p is a prime number will, at the most, be size $p - 1$.

For example $1/7 = 1 \div 7$. If we carry out the division a remainder of 1 will appear on the first division, a remainder of 1 will appear again after *six* divisions. We call this a cycle of size *six*.

However when we write $1/11$ in decimal form, the cycle starts again after two divisions. Note $p - 1 = 10$ and $2 | 10$.

So $1/p$ can have cycle length c where $c \leq p - 1$. It can be proved that $c | p - 1$.

- Fractions with composite denominators will have fixed and recurring parts if the denominators have a factor of 2 or 5 and a different number.

Examples:

$$1/14 = 0.07142857142857142857.. = 0.0\langle 714285 \rangle$$

$$1/36 = 0.02[7]$$

- with some exceptions, $1/p^2$ has an interesting rule for cycle size.

$$1/169 =$$

$$0.[005917159763313609467455621301775147928994082840236686390532544378698224852071]$$

This has cycle size 78 ($= 6 \times 13$).

These patterns which we have briefly outlined can be studied further by using the software from the above link.

| Fraction | Cycle size |
|---|-------------------|
| $1/3 = 0.[3]$ | 1 |
| $1/6 = 0.1[6]$ | 1 |
| $1/7 = 0.[142857]$ | 6 |
| $1/9 = 0.[1]$ | 1 |
| $1/11 = 0.[09]$ | 2 |
| $1/12 = 0.08[3]$ | 1 |
| $1/13 = 0.[076923]$ | 6 |
| $1/14 = 0.0[714285]$ | 6 |
| $1/15 = 0.0[6]$ | 1 |
| $1/17 = 0.[0588235294117647]$ | 16 |
| $1/18 = 0.0[5]$ | 1 |
| $1/19 = 0.[052631578947368421]$ | 18 |
| $1/23 = 0.[0434782608695652173913]$ | 22 |
| $1/29 = 0.[0344827586206896551724137931]$ | 28 |
| $1/31 = 0.[032258064516129]$ | 15 |
| $1/37 = 0.[027]$ | 3 |
| $1/41 = 0.[02439]$ | 5 |
| $1/43 = 0.[023255813953488372093]$ | 21 |
| $1/47 = 0.[0212765957446808510638297872340425531914893617]$ | 46 |
| $1/49 = 0.[020408163265306122448979591836734693877551]$ | 42 |
| $1/75 = 0.01[3]$ | 1 |
| $1/121 = 0.[0082644628099173553719]$ | 22 |

The Fibonacci Sequence

Some identities:

a) $\gcd(F_n, F_{n+1}) = 1$

b) $\gcd(F_n, F_m) = \gcd(n, m)$

c) $F_{m+n} = F_{m-1} F_n + F_m F_{n-1}$

d) $F_n^2 = F_{n+1} F_n - F_n F_{n-1}$

e) $F_{n+1} F_n = F_1^2 + F_2^2 + F_3^2 + \dots + F_n^2$

Exercises:

1) Show by induction or otherwise that $F_{m+n} = F_{m-1} F_n + F_m F_{n-1}$.

2) If $F_{10} = 55$, $F_{11} = 89$ and $F_{12} = 144$, using the above identity find F_{22} , F_{23} and F_{24} .

3) (a) Which Fibonacci numbers are multiples of 13?

(b) Show that 4 divides F_n , if and only if 8 divides F_n .

4) Prove that :

a. $F_1 + F_2 + F_3 + \dots + F_n = F_{n+2} - 1$.

b. $F_1 + F_3 + F_5 + \dots + F_{2n-1} = F_{2n}$.

5) Prove that if 3 divides F_n then 9 divides $F_{n+1}^3 - F_{n-1}^3$.

Appendix:

Fermat's Little Theorem [FLT]

- If p is prime and $\gcd(a, p) = 1$, then $a^{p-1} = 1 \pmod{p}$.

Example:

$4^{7-1} - 1 = 0 \pmod{7}$ i.e. FLT indicates that $4^{7-1} - 1$ should be divisible by 7.

$4^{7-1} - 1 = 4095$ and $4095 \div 7 = 585$.

Exercises:

1. Show $37^{37} + 2$ is divisible by 13
 - i. By using congruence properties
 - ii. By using FLT
2. Find the remainder when 11^{11} is divided by
 - i. 7
 - ii. 17
 - iii. 19
3. Use FLT to show that:
 - i. $3^{50} + 5^{50}$ is divisible by 17.
 - ii. $2^{100} + 3^{100}$ is divisible by 97.

Some Number Theory Terminology

- $a \mid b$: a divides into b ;

This is usually written as $b = 0 \pmod{a}$.

- $\gcd(a, b) = 1 \Rightarrow$ Greatest common divisor[highest common factor] of a & b is 1.

Also described as: a & b are coprime.

- $N = am + r$ where $0 \leq r < m \Rightarrow N$ has remainder r when divided by m .
- If $a \mid b$ and $a \mid c$ then $a \mid \lambda b + \mu c$.

Appendix:

Congruence

- a is **congruent** to b (modulo n) $\Leftrightarrow n|(a - b)$ or $a \div n$ and $b \div n$ have same remainder.
For example: $1 = 8 = 15 = 22 = -6 \pmod{7}$.
- $\{\dots - 6, 1, 8, 15, 22 \dots\}$ is an example of a **residue class** mod 7.
- **Properties:**
 - If $a = b \pmod{m}$ and if $a = b \pmod{n}$ then $a = b \pmod{mn}$ if $\gcd(m, n) = 1$.
e.g. $3 = 18 \pmod{3}$ and $3 = 18 \pmod{5} \Rightarrow 3 = 18 \pmod{15}$.
 - If $ca = cb \pmod{m}$ then $a = b \pmod{m/d}$ where d is $\gcd(c, m)$
 - It follows from above that if $ca = cb \pmod{m}$ then $a = b \pmod{m}$ when $\gcd(c, m) = 1$.
- **Solving linear congruences** i.e. equations of the form : $ax = b \pmod{n}$
 - Congruence has solutions if, and only if, $\gcd(a, n)$ divides b .
 - When $\gcd(a, n) = 1$, the congruence has a unique solution.
 - If $\gcd(a, n) = d$ and $d|b$, then the congruence has d solutions. The solutions are found by finding the unique solution to $-x = - \pmod{-}$.
- **Strategy for solving the linear congruence $ax = b \pmod{n}$:**
 1. Verify that $\gcd(a, n)$ divides b . If it does not then the congruence has no solutions.
 2. Cancel any common divisors of all three of a, b and n . The resulting coefficients can then be changed by using any of the following rules:
 3. Cancel any common divisor of the coefficients
 4. Replace any coefficient by any congruent number.
 5. Multiply through the congruence by any number **which is relatively prime to the modulus**.

Examples:

Solve the following linear congruences:

1) $8x = 12 \pmod{60}$

Solution: $2x = 3 \pmod{15}$ [$\gcd(8, 60) = 4 \Rightarrow 4$ solutions] $\Rightarrow 16x = 24 \pmod{15}$
 $\Rightarrow x = 9 \pmod{15} \Rightarrow x = 9, 24, 39, 54 \pmod{60}$.

2) $21x = 35 \pmod{47}$

Solution: $3x = 5 \pmod{47} \Rightarrow 48x = 80 \pmod{47} \Rightarrow x = 33 \pmod{47}$.

3) $6x = 5 \pmod{41}$

Solution: $42x = 35 \pmod{41} \Rightarrow x = 35 \pmod{41}$.