Mathematical Enrichment Feb 17th, 2018

Kevin Hutchinson: Number Theory

Two nonzero integers are relatively prime ("co-prime") if they have no common prime divisors:

Eg 6, 35

1, any number

p prime, any number not div. by p

Recall Euclid's trick. Given any integers $a_1, a_2, \dots, a_t$ we can find N which is rel. prime to all of them:

$$N = a_1 a_2 \cdots a_t + 1$$

or more generally

$$N = M a_1 \cdots a_t + 1$$ for any M.

(additional flexibility)

Eg

- Write down a ~~formula for~~ explicit description of an infinite sequence of numbers

$$b_1, b_2, b_3, \dots$$

Such that any pair are relatively prime:

$b_1 = 1,\ b_2 = 2,\ b_3 = 3, \dots$ and $b_{n+1} = b_1 \cdots b_n + 1$ for all n

Recall We adapted Euclid's argument to prove that there are infinitely many primes of the form $4n+3$.

Required: A product a numbers of the form $4n+1$ is again of the form $4n+1$.

Not true for numbers of the form $4n+3$:

We can't adapt this elementary argument to show that there are infinitely many primes of the form $4n+1$.

We'll prove, however that there are infinitely many primes of the form $4n+1$.

We use the following

Theorem Let p be an odd prime number.

Suppose p divides a number of the form

n^2+1.

Then p is of the form $4n+1$.

Proof Let $p_1, p_2, \dots, p_t$ be any finite list of primes of the form $4n+1$.

Consider $N = (p_1 \cdots p_t)^2 + 1$

$p_1, \dots, p_t$ don't divide N. By the Theorem, any prime divisor p of N is again of the form $4n+1$.

How do we prove the Theorem above.?

We'll use another famous theorem.

"Fermat's Little Theorem"

If p is a prime number then p divides $n^p - n$ for any $n \geq 1$.

[Exercise : Prove this by induction on n. Use the binomial theorem : Show if p is a prime then $p \mid \binom{p}{i}$ when $0 < i < p$].

Corollary If $p \nmid n$, then $p \mid n^{p-1} - 1$.

$$p \mid n^p - n = n \cdot (n^{p-1} - 1)$$

and it follows from fundamental property of prime numbers: if $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Theorem Let p be an odd prime. Suppose $p \mid k^2 + 1$ for some integer k. Then p is of the form $4u+1$.

Proof: $p \mid k^2 + 1 \Longrightarrow \ell p = k^2 + 1$ for some integer ℓ.

So $k^2 = \ell p - 1$.

$$p \nmid k \quad \Rightarrow \quad p \mid k^{p-1} - 1$$

$$\Rightarrow \quad mp = k^{p-1} - 1 \qquad \text{for some } m.$$

(by Corollary).

$$\text{So} \quad mp = (k^2)^{\frac{p-1}{2}} - 1$$

$$= (k^2)^{r} - 1 \qquad \text{where } r = \frac{p-1}{2}$$

$$= (\ell p - 1)^r - 1$$

$$= \underbrace{(\ell p)^r - r\cdot(\ell p)^{r-1} + \binom{r}{2}(\ell p)^{r-2} -}\ + (-1)^r - 1$$

$$mp = px + (-1)^r - 1 \qquad \text{for some integer } x$$

$$\Rightarrow \quad (-1)^r - 1 = p(m - x)$$

$$\text{So} \quad p \mid (-1)^r - 1 \qquad \text{and} \quad p > 2$$

$$\Rightarrow \quad r \text{ is even}$$

$$\Rightarrow \quad \frac{p-1}{2} \text{ is even}$$

$$\Rightarrow \quad \frac{p-1}{2} = 2n \qquad \text{for some } n$$

$$\Rightarrow \quad p - 1 = 4n$$

$$\Rightarrow \quad \boxed{p = 4n + 1.}$$

Another famous theorem in number theory

"Dirichlet's Thearem on primes in arithmetic progressions"

Arithmetic progression with 1st term a and common difference d is the sequence

$$a,\ a+d,\ a+2d, \ldots, a+nd, \ldots$$

eg: if $a=1, d=4$, get $4n+1$

if $a=3, d=4$ get $4n+3$.

If $a=5, d=8$, get $8n+5$

$5, 13, 21, 29, \ldots$

Thearem

In any arithmetic progression $a+nd$ in which a, d are relatively prime, there are infinitely many primes.

eg. There are inf. many primes of the form $8n+5$

. . . . $7n+3$

. . . . $13n+4$

$\vdots$

etc

Recall:

Can one find 14 consecutive integers such that each is divisible by at least one of the primes 2, 3, 5, 7, 11.

Answer No. Let's prove this.

Take any 14 consecutive integers..

Let $a_1 < a_2 < a_3 \quad \cdots \quad < a_7$

be the odd numbers among them.

So $a_{i+1} = a_i + 2$ for $i = 1, .., 6$

$\therefore$ If $3 | a_i$ then $3 \nmid \underset{a_i+2}{\underset{\shortparallel}{a_{i+1}}}$, $3 \nmid \underset{a_i+4}{\underset{\shortparallel}{a_{i+2}}}$

Thus 3 divides at most $\boxed{\underline{3}}$ of them (and if it divides three of them, they must be

$$a_1 \qquad a_4 \qquad a_7$$

Likewise, if $5 | a_i$, $5 \nmid a_{i+1}, .. a_{i+4}$.

So 5 divides at most $\boxed{\underline{\underline{2}}}$

7 divides at most $\boxed{\underline{1}}$

11 divides at most $\boxed{1}$

Since $3+2+1+1 = 7$

the only way that each a_i is divisible by at least one of $3, 5, 7, 11$ only if each maximum possible is achieved, with no overlaps.

So a_1, a_4, a_7 are divisible by 3.

Two are div by 5. ← at least a distance 10 apart.

$a_6 - a_2 = 8$ is too small.

So this is impossible and therefore at least one of the a_i's is not divisible by $2, 3, 5, 7$ or 11. (U.S.A Math Olymp. problem).

Part 2 of the problem.

Show there are 13 consecutive integers with the property that each is divisible by at least one of $2, 3, 5, 7, 11$.

Solution. I claim there is a number N with the following properties:

(a) N leaves remainder 0 on division by 30
(b) N 1 7
(c) N . . . . . . 10 . . . . . 11.
↑ rel. prime.

[Proof "Chinese Remainder Theorem"].

$$\overbrace{N-6, \quad \ldots,}^{\text{div. 2, 3, 5.}} \underset{\substack{\uparrow \\ \text{div } 7}}{N-1}, \underset{\substack{\uparrow \\ \text{div by } 2,3,5}}{N}, \underset{\substack{\uparrow \\ \text{div } 11}}{N+1}, \overbrace{\ldots, N+6,}^{\text{div by 2, 3 or 5}}$$

Exercise (a) Show there no 22 consecutive integers each of which is div by at least one of 2, 3, 5, 7, 11, 13.

(b) Show there are 21 consecutive ints each div by at least of 2, 3, 5, 7, 11, 13.

Chinese Remainder Theorem

If $m_1, \ldots, m_t$ are relatively prime in pairs.

Take any numbers $a_1, \ldots, a_t$, $\left(\begin{array}{l} 0 \le a_1 \le m_1 \\ 0 \le a_2 < m_2 \\ \quad \vdots \end{array}\right)$

Then there is a number N satisfying

N leaves remainder a_1 on div by m_1

a_2 - - m_2

$\vdots \qquad \vdots \qquad \vdots$

a_t - - - m_t

(and a recipe to find N).