3 More on divisibility and Primes

Proposition 1: Let $a_1, a_2, \dots, a_n$ be integers. Put

$$M = \{\sum_{i=1}^{n} a_i x^i | x_i \in \mathbb{Z}, \forall i\}.$$

Then $M = d\mathbb{Z}$, for a unique $d \geq 0$. ($d\mathbb{Z}$ is the set of all integers divisible by d.)

Proof. Certainly, $D \in M$. If $M = \{0\}$, take $d = 0$. Otherwise, put $M^+ = \{n \in M | n > 0\}$. Then clearly, M^+ is non-empty since $M \neq \{0\}$, and so by WOA, $\exists$ smallest element, call it d, in M^+. For any n in M, we can write by the Euclidean algorithm: $n = dq + r$, with $q, r \in \mathbb{Z}$, and $0 \leq r < d$.

Note that M is closed under subtraction. So $r = n - dq$ is also in M. If $r = 0$, we are done because then $n = dq$ as desired.

Suppose $r > 0$. Then $r \in M^+$. Since $r < d$, this contradicts the minimality of d. Hence r must be 0, and $n \in d\mathbb{Z}$.

Definition: Let $a_1, \dots, a_n, d$ be as in Prop. 1. Then d is called the gcd (**greatest common divisor**) of $\{a_i\}$. For brevity, write

$$d = (a_1, \dots, a_n) = gcd(a_1, \dots, a_n).$$

Check: $(a_1, (a_2, a_3)) = ((a_1, a_2), a_3)$

Definition: $\{a_i\}$ are mutually relatively prime iff $(a_1, \dots, a_n) = 1$.

Example: (2,3,9) is mutually relatively prime but not *pairwise* relatively prime.

Proposition 2. $a_1, \dots, a_n$ are mutually relatively prime iff we can solve the equation

$$\sum_{i=1}^{n} a_i x_i = 1 \qquad (*)$$

in integers.

Proof. Suppose $d = (a_1, \dots, a_n) = 1$. Then by Prop.1, $1 = d \in M = \{\sum_{i=1}^{n} a_i x^i | x^i \in \mathbb{Z}\}$. So (*) can be solved in integers. Conversely, suppose

(*) has a solution in integers. Then $1 \in M^+$, and so $d = 1$.

Proposition 3. Let $a, b, c \in \mathbb{Z}$, $(a, b) = 1$. Suppose $a|bc$. Then $a|c$.

Proof. Since $(a, b) = 1$, by Prop.2, $\exists\ x, y \in \mathbb{Z}$. Set $ax + by = 1$. Then $c = c(ax + by) = a(cx) + (bc)y$. Since $a|bc$, a divides the right hand side, hence $a|c$.

Proof of unique factorization in $\mathbb{Z}$.

Existence

As shown before, every $n \geq 1$ is a product of primes.

Uniqueness (second proof)

Let $n > 1$ be the smallest counterexample. So we can write $n = p_1 \dots p_r = q_1 \dots q_s$, with p_i, q_j primes and $p_1 \neq q_j$ for any (i, j). So

$$p_1 | n = q_1 \dots q_s = q_1(q_2 \dots q_s).$$

Since $p_1 \neq q_1$, $(p_1, q_1) = 1$, and by Prop. 3, $p_1|(q_2 \dots q_s)$. Again, since $p_1 \neq q_2$, applying Prop.3 again, $p_1|(q_3 \dots q_s)$. Finally get $p_1|q_s$. So there is no such counterexample.

Third Proof of the Infinitude of Primes in $\mathbb{Z}$ (Polya)

For every $n \geq 1$, put $F_n = 2^{2^n} + 1$, called the nth *Fermat number*.

Lemma. If $n \neq m$, $(F_n, F_m) = 1$.

Proof of Lemma. We may assume $m > n$. Write $m = n + k$, for some $k > 0$. *To show*:

$$(F_n, F_{n+k}) = 1 \quad (\text{for } k > 0.)$$

Suppose $d|F_n$ **and** $d|F_{n+k}$. Put $x = 2^{2^n}$. Then, since

$$F_{n+k} = 2^{2^{n+k}} + 1 = 2^{2^n 2^k} + 1,$$

$$\begin{aligned} \frac{F_{n+k} - 2}{F_n} &= \frac{x^{2^k} - 1}{x + 1} \\ &= x^{2^k - 1} - x^{2^k - 2} + \cdots - 1 \in \mathbb{Z} \end{aligned}$$

$$\Rightarrow F_n|(F_{n+l}-2) \Rightarrow d|2.$$

But F_n, F_{n+k} are odd. So $d=1$. Hence the lemma.

Proof of Infinitude of primes

Consider $F_1, F_2, \ldots, F_n \ldots$ By lemma, each F_n is divisible by a prime, call it p_n, not dividing the previous $F_k,\ k<n$. The sequence $\{p_1, p_2, \ldots\}$ is infinite.

One has: $F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537$ (Fermat), $F_5 = (641)(6700417), \ldots$

Primes in "Arithmetic Progressions":

Fix $m>1$, and $a \in \mathbb{Z}$ such that $(a,m)=1$.

Theorem (Dirichlet) $\exists$ infinitely many primes p which are $\equiv a \pmod{m}$.

We cannot possibly prove it in this class. But we can prove the following:

Baby Lemma $\exists$ infinitely many primes p which are $\equiv 3 \pmod 4$.

Proof: Suppose $\exists$ only a finite number of such primes, say 3, p_1, p_2, $\cdots$, p_r.

Consider

$$N = 4p_1\,p_2\,\cdots p_r + 3.$$

By unique factorization in $\mathbb{Z}$ we can write $N = q_1 q_2 \cdots q_s$, with the q_j's being primes.

Claim 1: Some q_j must be $\equiv 3(mod\,4)$.

Indeed, every q_j is an odd prime as N is odd, and moreover if $q_j \equiv 1 \pmod 4$ $\forall_j$, then N will also be $\equiv 1 \pmod 4$, contradiction! Hence Claim 1.

Say $q_1 \equiv 3 \pmod 4$.

Claim 2: $q_1 \notin \{3, p_1, \cdots, p_r\}$.

Indeed, if $q_1 = 3$, then $3|N$, and since $N = 4p_1 \cdots p_r + 3$, 3 must divide $4p_1 \cdots p_r, \rightarrow\leftarrow$. So $q_1 \neq 3$. Suppose $q_1 = p_i$ for some $1 \leq i \leq r$. Then $p_i \mid N$, and since $N = 4p_1 \cdots p_r + 3$, $p_i \mid 3$, $\rightarrow\leftarrow$. So $q_1 \neq p_i$. Hence Claim 2.

So we have produced a new prime $q_1 \equiv 3 \pmod 4$ which is not in the original list, $\rightarrow\leftarrow$.

Remark: There is no such simple argument to prove Dirichlet's theorem for primes $\equiv 1 \pmod 4$. We can try to start the same way by assuming that we have a finite list of primes $\equiv 1 \pmod 4$, say $p_1, p_2, \cdots, p_r$, and we can consider $N = 4p_1 \cdots p_r + 1$. Factor N as $q_1 \cdots q_s$. Now the analog of Claim 1 will in general fail as the product of an even number of numbers congruent to 3 (mod 4) is 1 (mod 4). However, we will prove the infinitude of such primes later after studying squares mod p.

Earlier we saw a *heuristic reason* for expecting there to be an infinite number of **twin primes**, e.g. $\{3, 5\}$, $\{5, 7\}$, $\{11, 13\}, \cdots$
Expectation:

$$\pi_2(x) := \# \begin{pmatrix} \text{twin primes} \\ \leq x \end{pmatrix} \approx \quad C\,\frac{x}{\log^2 x}, \qquad \text{as } x \to \infty.$$

This means $\pi_2(x) - \frac{cx}{\log^2 x}$ goes to 0 as x goes to ∞.

This twin prime problem is closely related to the **Goldbach problem**, which asks if every even number ≥ 4 is a sum of 2 primes.
Best known result: (Chen)

$$2n = a_1 + a_2, \text{ with } a_i \text{ prime or a product of 2 primes.}$$

A similar heuristic reason makes one expect that there are infinitely many primes p of the form $n^2 + 1$.
Best known result: (Iwaniec)

$$\exists \text{ an infinite of sequence } \{m_1, m_2, \cdots\}$$

such that

(i)

$$m_j = n_j^2 + 1, \qquad \forall j$$

and for every j,

(ii)

$$m_j \text{ is a prime or a product of 2 primes}$$

The proof is quite hard and beyond the scope of our class.