Tuesday, March 22, 2016 1:24 PM

Prime numbers form one of the amazing sequences of integers. They have a lot of, in the first glance, contradictory properties which makes them mysterious.

- In many aspects they behave similar to "random" integers. (A "low complexity" function would not have correlation with Möbius function (it will be defined soon.))
- Primes are "more or less independent", but we have reciprocity law(s).

There are a lot of conjectures or theorems that ask for primes in certain sequence of integers:

<u>Thm (Dirichlet)</u> Suppose $\gcd(a,b)=1$. Then there are infinitely many primes of the form $ak+b$.

<u>Twin prime conj.</u> $\exists \infty$ $n \in \mathbb{Z}$, n and $n+2$ are prime.

<u>Euler's conj.</u> $\exists \infty$ $n \in \mathbb{Z}$, n^2+1 is prime.

One of the main reasons that we are interested in primes is because of unique factorization property of integers:

Any integer $n>1$ can be written as a product of primes in a unique way.

So for any prime p, there is a well-defined function

$$v_p : \mathbb{Z}^{>1} \longrightarrow \mathbb{Z}^{\geq 0} \quad \text{s.t.} \quad n = \prod_{p:\text{prime}} p^{v_p(n)} .$$

Notice that, for any n, except for finitely many primes $v_p(n)=0$ and so the above product has only finitely many terms that are not 1.

We can easily extend these to $\underline{\mathbb{Q}\setminus\{0\}}$. So we get

$v_p : \mathbb{Q}^\times \longrightarrow \mathbb{Z}$, s.t. $\forall \frac{m}{n} \in \mathbb{Q}^\times$,

$$\left|\frac{m}{n}\right| = \prod_{p\in\mathcal{P}} p^{v_p(\frac{m}{n})}.$$

Let's also assume $v_p(0) = \infty$ (This way we do not have add extra conditions.)

v_p is called <u>the p-adic valuation of $\mathbb{Q}$</u>.

<u>Basic properties of v_p.</u>

① $\forall q_1, q_2 \in \mathbb{Q}$, $v_p(q_1 q_2) = v_p(q_1) + v_p(q_2)$.

② $\forall p \in \mathcal{P}$, $v_p(q) \geq 0 \Rightarrow q \in \mathbb{Z}$.

③ $0 \neq m \in \mathbb{Z}, n \in \mathbb{Z}$; $\forall p \in \mathcal{P}$, $v_p(m) \leq v_p(n) \Longleftrightarrow m \mid n$.

④ $\forall q_1, q_2 \in \mathbb{Q}$, $v_p(q_1 + q_2) \geq \min\{v_p(q_1), v_p(q_2)\}$.

<u>Proof.</u>
- $\left.\begin{array}{l} |q_1| = \prod_{p\in\mathcal{P}} p^{v_p(q_1)} \\ |q_2| = \prod_{p\in\mathcal{P}} p^{v_p(q_2)} \end{array}\right\} \Rightarrow |q_1 q_2| = \prod_{p\in\mathcal{P}} p^{v_p(q_1)+v_p(q_2)}$

  $\Rightarrow v_p(q_1 q_2) = v_p(q_1) + v_p(q_2)$.

- $q \in \mathbb{Q} \Rightarrow \exists\, m, n \in \mathbb{Z}^+$ s.t. $\gcd(m,n) = 1$ and $|q| = \frac{m}{n}$.

  If $q \notin \mathbb{Z} \Rightarrow n \neq 1 \Rightarrow \left.\begin{array}{l} \exists\, p \in \mathcal{P}, p \mid n \\ \gcd(m,n) = 1 \end{array}\right\} \Rightarrow p \nmid m$

  $\Rightarrow v_p(n) > 0$ and $v_p(m) = 0$

  $\Rightarrow v_p\left(\frac{m}{n}\right) = v_p(m) - v_p(n) < 0$, which is a contradiction.

- $(\Rightarrow)$ $\forall p \in \mathcal{P}$, $v_p\left(\frac{n}{m}\right) = v_p(n) - v_p(m) \geq 0$

  $\Rightarrow \frac{n}{m} \in \mathbb{Z} \Rightarrow m \mid n$.

$\forall$

$(\Leftarrow)\quad m|n \Rightarrow \frac{n}{m}\in\mathbb{Z} \Rightarrow \forall p\in\mathcal{P},\ v_p(\frac{n}{m})\geq 0$

$$\Rightarrow \forall p\in\mathcal{P},\ v_p(m)\leq v_p(n).$$

•

Let $n_1=\prod_p p^{v_p(q_1)-\min(v_p(q_1),v_p(q_2))}\in\mathbb{Z}^{\geq 1}$

and $n_2=\prod_p p^{v_p(q_2)-\min(v_p(q_1),v_p(q_2))}\in\mathbb{Z}^{\geq 1}$.

$$\Rightarrow q_1+q_2=\pm\prod_p p^{v_p(q_1)}\pm\prod_p p^{v_p(q_2)}$$

$$=\prod_p p^{\min(v_p(q_1),v_p(q_2))}\underbrace{(\pm n_1\pm n_2)}_{\in\mathbb{Z}}$$

$$\Rightarrow v_p(q_1+q_2)=\min(v_p(q_1),v_p(q_2))+\underbrace{v_p(\pm n_1\pm n_2)}_{\geq 0}$$

$$\geq \min(v_p(q_1),v_p(q_2)).\qquad \blacksquare$$

<u>Corollary</u>. $\forall m,n\in\mathbb{Z}^+$, • $v_p(\gcd(m,n))=\min(v_p(m),v_p(n))$

• $v_p(\mathrm{lcm}(m,n))=\max(v_p(m),v_p(n))$

• $m\cdot n=\gcd(m,n)\cdot\mathrm{lcm}(m,n)$

<u>Proof</u>. (exercise)

There are a lot of interesting functions on $\mathbb{Z}$ that almost preserve its multiplicative structure.

<u>Definition</u>. A function $f:\mathbb{Z}^+\to\mathbb{C}$ is called a <u>multiplicative function</u> if ① $f(1)=1$.

② $\gcd(m,n)=1\Rightarrow f(mn)=f(m)\cdot f(n)$.

Let $\mathcal{M}$ be the set of all multiplicative functions.

<u>Ex.</u>. $\mathbb{1}:\mathbb{Z}^+\to\mathbb{C}$, $\mathbb{1}(n)=1$ constant function.

• $\mathrm{id}.:\mathbb{Z}^+\to\mathbb{C}$, $\mathrm{id}.(n)=n$ the identity function.

• $I:\mathbb{Z}^+\to\mathbb{C}$, $I(n)=\begin{cases}1 & n=1\\ 0 & n\neq 1\end{cases}$

$\begin{cases} 0 & n \neq 1 \end{cases}$

- $n \mapsto n^s$ for any real number s.

<u>Observation</u>. Any function on powers of primes can be uniquely extended to a multiplicative function:

$$f(n) := \prod_{p \in \mathcal{P}} f(p^{v_p(n)}).$$

Again notice that, since $f(1)=1$, this product has only finitely many terms that are not 1.

<u>Definition</u> (Multiplicative convolution) For any two arithmetic functions $f, g : \mathbb{Z}^+ \to \mathbb{C}$, let

$$(f * g)(n) := \sum_{d \mid n} f(d)\, g\left(\frac{n}{d}\right).$$

<u>Basic properties.</u>

(Commutative) $f * g = g * f$

<u>Pf</u>. $(f * g)(n) = \sum_{d_1 d_2 = n} f(d_1)\, g(d_2)$

$$= \sum_{d_2 d_1 = n} g(d_2)\, f(d_1) = (g * f)(n).$$

(Associative) $(f * g) * h = f * (g * h)$

<u>Pf</u>. One can easily see that $((f * g) * h)(n)$ and $(f * (g * h))(n)$ are equal to

$$\sum_{d_1 d_2 d_3 = n} f(d_1)\, g(d_2)\, h(d_3).$$

(Nuetral element) $I * f = f * I = f$

<u>Pf.</u> $(I * f)(n) = \sum_{d \mid n} I(d)\, f\left(\frac{n}{d}\right) = I(1) f(n) = f(n)$.

(Invertible elements) Suppose $f(1) = 1$. Then $\exists !\, g : \mathbb{Z}^+ \to \mathbb{C}$

(Invertible elements) Suppose $f(1)=1$. Then $\exists !\, g:\mathbb{Z}^+\to\mathbb{C}$ s.t. $f*g=g*f=I$.

Pf. We define g recursively so that

$$(f*g)(n)=I(n).$$

Let $g(1)=1$ and for any $n\in\mathbb{Z}^{>1}$

$$g(n)=-\sum_{\substack{d\mid n\\ d\neq 1}} f(d)\, g(\tfrac{n}{d}).$$

This shows existence and uniquess.

Theorem ① $f,g\in\mathcal{M}\Rightarrow f*g\in\mathcal{M}$

② $f\in\mathcal{M}\Rightarrow f^{-1}\in\mathcal{M}$ (inverse with respect to $*$)

Proof. ① Suppose $\gcd(m,n)=1$.

$$(f*g)(mn)=\sum_{d\mid mn} f(d)\, g(\tfrac{mn}{d})$$

- $\forall\, d\mid mn$, let $d_1=\prod_{v_p(m)>0} p^{v_p(d)}$ and $d_2=\prod_{v_p(n)>0} p^{v_p(d)}$

Since $\gcd(m,n)=1\Rightarrow \forall p\in\mathcal{P}$, either $v_p(m)=0$ or $v_p(n)=0$, we have $d=d_1d_2$, $d_1\mid m$ and $d_2\mid n$.

In fact this gives us a bijection between

$\{d\mid d \text{ divides } mn\}$ and $\{d_1\mid d_1 \text{ divides } m\}\times\{d_2\mid d_2 \text{ divides } n\}$

So $$(f*g)(mn)=\sum_{\substack{d_1\mid m\\ d_2\mid n}} f(d_1d_2)\, g(\tfrac{m}{d_1}\cdot\tfrac{n}{d_2}).$$

Since $\gcd(m,n)=1$, $\gcd(d_1,d_2)=\gcd(\frac{m}{d_1},\frac{n}{d_2})=1$.

Hence $$(f*g)(mn)=\sum f(d_1)\, f(d_2)\, g(\tfrac{m}{1})\, g(\tfrac{n}{1})$$

Hence $\quad (f*g)(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)\, f(d_2)\, g(\frac{m}{d_1})\, g(\frac{n}{d_2})$

$$= \Big(\sum_{d_1|m} f(d_1) g(\tfrac{m}{d_1})\Big)\Big(\sum_{d_2|n} f(d_2) g(\tfrac{n}{d_2})\Big)$$

$$= (f*g)(m)\ (f*g)(n).$$

② Let $g = f^{-1}$. So $(f*g)(n) = I(n)$.

By strong induction on $\underline{mn}$, we show that

$g(mn) = g(m)\, g(n)$ if $\gcd(m,n) = 1$.

By the definition of g we have:

$$g(mn) = -\sum_{\substack{d|mn \\ d \neq mn}} f(d)\, g(\tfrac{mn}{d})$$

above discussion

$$= -\sum_{\substack{d_1|m \\ d_2|n \\ \text{either } d_1 \neq 1 \\ \text{or } d_2 \neq 1}} f(d_1 d_2)\, g(\tfrac{m}{d_1} \cdot \tfrac{n}{d_2})$$

strong induction hypothesis

$$= -\sum_{\substack{d_1|m \\ d_2|n \\ \text{either } d_1 \neq 1 \\ \text{or } d_2 \neq 1}} f(d_1)\, f(d_2)\, g(\tfrac{m}{d_1})\, g(\tfrac{n}{d_2})$$

$$= -\sum_{\substack{d_2|n \\ d_2 \neq 1}} f(1) f(d_2) g(m) g(\tfrac{n}{d_2}) - \sum_{\substack{d_1|m \\ d_1 \neq 1}} f(d_1) f(1) g(\tfrac{m}{d_1}) g(n)$$

$$-\Big(\sum_{\substack{d_1|m \\ d_1 \neq 1}} f(d_1) g(\tfrac{m}{d_1})\Big)\Big(\sum_{\substack{d_2|n \\ d_2 \neq 1}} f(d_2) g(\tfrac{n}{d_2})\Big)$$

$$= g(m)\,g(n) + g(m)\,g(n) - g(m)\,g(n)$$

$$= g(m)\, g(n). \qquad \blacksquare$$

Corollary. $(\mathcal{M}, *)$ is an abelian group.

Ex. $\mathbb{1} * \mathbb{1} \in \mathcal{M}$;

$$(\mathbb{1} * \mathbb{1})(n) = \sum_{d \mid n} 1 = \#\text{ of positive divisors of } n$$
$$=: \tau(n).$$

$$\Rightarrow \tau(n) = \prod_p \tau(p^{v_p(n)}) = \prod_p (v_p(n)+1).$$

Ex. $\mathbb{1} * \mathrm{id}. \in \mathcal{M}$;

$$(\mathbb{1} * \mathrm{id}.)(n) = \sum_{d \mid n} d = \text{sum of positive divisors}$$
$$=: \sigma(n)$$

$$\Rightarrow \sigma(n) = \prod_p \sigma(p^{v_p(n)}) = \prod_p (1 + p + \cdots + p^{v_p(n)})$$
$$= \prod_p \frac{p^{v_p(n)} - 1}{p-1}.$$

Lemma. Let $\mu = \mathbb{1}^{-1}$ be the inverse of the constant function with respect to $*$. Then

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & \exists p,\ v_p(n) > 1. \\ (-1)^s & \text{if } n = p_1 \cdots p_s \text{ and } p_i \neq p_j. \end{cases}$$

Pf. We proceed by strong induction:

- $\mu(1) = 1 \Rightarrow$ base ✓

- $$\mu(n) = -\sum_{\substack{d \mid n \\ d \neq n}} \mu(d).$$

Suppose $v_{p_0}(n) \geq 2$. Then by strong induction hypoth.

$$\mu(n) = -\sum_{d \mid (n/p_0)} \mu(d) = -(\mathbb{1} * \mu)(n/p_0)$$
$$= -I(n/p_0) = 0.$$

Suppose $n = p_1 \cdot p_2 \cdots p_s$ and $p_i \neq p_j$.

$$\mu(n) = -\sum_{d \mid n} \mu(d) - \sum_{\substack{d \mid n \\ p}} \mu(d)$$

$$= -\sum_{d \mid n/p_1} \mu(d) + \sum_{\substack{d' \mid n/p_1 \\ d' \neq n/p_1}} \mu(d')$$

$$\underbrace{\qquad\qquad}_{(\mathbb{1} * \mu)(n/p_1)} \qquad \underbrace{\qquad\qquad}_{\text{if } n \neq p_1}$$

- if $\underline{n = p_1}$, then $\mu(p_1) = -1$.
- if $\underline{n \neq p_1}$, then $\mu(n) = -\mu(n/p_1) = -(-1)^{s-1} = (-1)^s$.

$\blacksquare$

Definition μ is called the <u>Möbius function</u>.

Corollary (Möbius inversion).

For $f : \mathbb{Z}^{\geq 1} \to \mathbb{C}$, let $F(n) = \sum_{d \mid n} f(d)$. Then

$$f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) F(d).$$

Moreover $f \in \mathcal{M} \iff F \in \mathcal{M}$.

Proof. $F = f * \mathbb{1} \Rightarrow F * \mu = (f * \mathbb{1}) * \mu$

$$= f * (\mathbb{1} * \mu)$$
$$= f * I$$
$$= f.$$

- $\left.\begin{matrix} f \in \mathcal{M} \\ \mathbb{1} \in \mathcal{M} \end{matrix}\right\} \Rightarrow F = f * \mathbb{1} \in \mathcal{M}.$

- $\left.\begin{matrix} F = f * \mathbb{1} \in \mathcal{M} \\ \mu \in \mathcal{M} \end{matrix}\right\} \Rightarrow f = F * \mu \in \mathcal{M}.$

$\blacksquare$

Recall. The Euler ϕ-function

$$\phi(n) := |\{ a \in \mathbb{Z}^{\geq 1} \mid a \leq n, \ \gcd(a,n) = 1 \}|$$
$$= |(\mathbb{Z}/n\mathbb{Z})^{\times}|.$$

Theorem ① $\phi \in \mathcal{M}$

Theorem ① $\phi \in \mathcal{M}$

② $\phi * \mathbb{1} = id.$

Proof. ① By Chinese Remainder Theorem, $\mathbb{Z}/_{mn\mathbb{Z}} \simeq \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$

if $\gcd(m,n) = 1$. So

$$\left(\mathbb{Z}/_{mn\mathbb{Z}}\right)^{\times} \simeq \left(\mathbb{Z}/_{m\mathbb{Z}}\right)^{\times} \times \left(\mathbb{Z}/_{n\mathbb{Z}}\right)^{\times}$$

$\Rightarrow \phi(mn) = \phi(m)\phi(n).$

② $$\{1, 2, \cdots, n\} = \bigsqcup_{d|n} \{k \mid 1 \leq k \leq n, \ \gcd(k,n) = d\}$$

$$= \bigsqcup_{d|n} \{dk' \mid 1 \leq k' \leq n/_d, \ \gcd(k', \tfrac{n}{d}) = 1\}$$

$$\Rightarrow n = \sum_{d|n} \phi\left(\frac{n}{d}\right) = (\mathbb{1} * \phi)(n).$$ ■

Corollary. $\phi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d.$

Pf. $id. = \phi * \mathbb{1} \Rightarrow \phi = id. * \mu.$ ■