MATH 113: DISCRETE STRUCTURES
FRIDAY WEEK 13 HANDOUT

Suppose $n = p_1^{a_1} \cdots p_k^{a_k}$ for positive integers a_i and distinct primes p_i. Recall that $\phi(n)$ is the number of positive integers smaller than n and relatively prime to n. We claim that

$$\phi(n) = n(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k).$$

To prove this, we count the number of positive integers which are at most n and are not relatively prime to n. This is the case if and only if one of the p_i divides n. Of course, there are n/p_i positive integers $\leq n$ and divisible by p_i, so it is tempting to guess that $\phi(n) = n-(n/p_1+n/p_2+\cdots+n/p_k)$, but inclusion-exclusion tells us we need to be more careful with numbers which are divisible by multiple primes. The correct formula is

$$\phi(n) = n - \sum_{1 \leq i \leq k} \frac{n}{p_i} + \sum_{1 \leq i_1 < i_2 \leq k} \frac{n}{p_{i_1} p_{i_2}} - \sum_{1 \leq i_1 < i_2 < i_3 \leq k} \frac{n}{p_{i_1} p_{i_2} p_{i_3}} + \cdots \pm \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}}$$

where the signs alternate and the final sign is $+$ if k is even and $-$ if k is odd. Factoring out an n and thinking deeply about the distributive law, we see that this is the same as

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

What a remarkable formula! For instance, if $n = 6160 = 2^3 \cdot 5^2 \cdot 7 \cdot 11$, then

$$\phi(6160) = 6160(1 - 1/2)(1 - 1/3)(1 - 1/5)(1 - 1/7)(1 - 1/11) = 1280.$$

Also note that there is a probabilistic interpretation of this formula. The probability that an integer between 1 and n is relatively prime to n is

$$\frac{\phi(n)}{n} = \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Fascinatingly, the probability only depends on the primes dividing n, and it suggests an alternate proof of our formula.

Problem 1. Let $\underline{n}$ be our sample space with uniform distribution. Define the event ND_i to be the set of $r \in \underline{n}$ such that $p_i \nmid r$.

(a) What is $P(ND_i)$?
(b) Let RP be the collection of $r \in \underline{n}$ which are relatively prime to n. Check that $RP = ND_1 \cap ND_2 \cap \cdots \cap ND_k$.
(c) Argue that the events ND_i are independent and thus $P(RP) = P(ND_1) \cdots P(ND_k)$. Note that this is equivalent to the above formula for $\phi(n)$.

Here's another application of probability theory to number theory, due to Erdős (1965). Call $S \subseteq \mathbb{Z}$ *sum free* if for all $a, b, c \in S$, $a + b \neq c$.

Theorem 2. *Let A be a finite set of nonzero integers. Then there exists $S \subseteq A$ which is sum free with size $|S| > |A|/3$.*

Proof. Choose a prime number $p = 3k + 2$, where k is large enough that $A \subseteq [-p/3, p/3] \smallsetminus \{0\}$. Reduce everything in A modulo p to produce $\overline{A} = \{\overline{a} \mid a \in A\} \subseteq \mathbb{Z}/p\mathbb{Z}$. Because of how we chose k, $|A| = |\overline{A}|$. Observe (*i.e.* check!) that a subset $\overline{S}$ of $\overline{A}$ will be sum free if and only if the corresponding $S \subseteq A$ is sum free.

Now randomly choose $\overline{x} \in \mathbb{Z}/p\mathbb{Z}^\times$ uniformly, and form the set

$$\overline{S}_{\overline{x}} = \overline{A} \cap (\overline{x} \cdot \overline{[k+1, 2k+1]}) = \{\overline{a} \in A \mid \overline{x}^{-1}\overline{a} \in \{\overline{k+1}, \ldots, \overline{2k+1}\}.$$

Since $\overline{[k+1, 2k+1]}$ is sum free in $\mathbb{Z}/p\mathbb{Z}$, we see that $\overline{x} \cdot \overline{[k+1, 2k+1]}$ is too, and thus $\overline{S}_{\overline{x}}$ is sum free. It now suffices to show that $\overline{S}_{\overline{x}}$ has cardinality greater than $|A|/3$ with positive probability. Viewing $|\overline{S}_{\overline{x}}|$ as a random variable on $\mathbb{Z}/p\mathbb{Z}^\times$, it suffices to prove that $E(|\overline{S}_{\overline{x}}|) > |A|/3$.

Via the method of indicator variables, we may compute

$$E(|\overline{S}_{\overline{x}}|) = \sum_{a \in A} P(\overline{a} \in \overline{S}_{\overline{x}}) = \sum_{a \in A} P(\overline{x}^{-1}\overline{a} \in \overline{[k+1, 2k+1]}).$$

Since $\overline{a}$ is invertible in $\mathbb{Z}/p\mathbb{Z}$, multiplication by $\overline{a}$ is a bijection $\mathbb{Z}/p\mathbb{Z}^\times \to \mathbb{Z}/p\mathbb{Z}^\times$. It follows that $\overline{x}^{-1}\overline{a}$ is uniformly randomly distributed in $\mathbb{Z}/p\mathbb{Z}^\times$. Since $|\overline{[k+1, 2k+1]}| > \frac{p-1}{3}$, we conclude that $P(\overline{x}^{-1}\overline{a} \in \overline{[k+1, 2k+1]}) > 1/3$ for all $a \in A$. Thus $E(|\overline{S}_{\overline{x}}|) > |A|/3$, as desired. $\square$