Lecture 15
Linear Recurrences

Proof of 4. from last time, that probability of any two positive integers at random are relatively prime is $\frac{6}{\pi^2}$. ie., that

$$\lim_{N\to\infty} \frac{|\{(x,y) \in \{1\dots N\} \times \{1\dots N\} : (x,y) = 1\}|}{N^2} = \frac{6}{\pi^2}$$

Why? If x, y random, fixed prime p, probability that p divides x is $\frac{1}{p}$, so probability divides both is $\frac{1}{p^2}$, with complement $1 - \frac{1}{p^2}$. $\prod_{p \text{ prime}}(1 - \frac{1}{p^2})$ is the probability that no prime divides both x, y, which means x, y are coprime.

Proof of 5. from last time - with a, b random, the probability that their gcd is n has to be of the form $\frac{c}{n^2}$ for some constant c.

$$(a,b) \Rightarrow a = na', b = nb'$$

$$\begin{aligned}
(a',b') &= 1 \\
&\Rightarrow P((a,b) = n) = \frac{6}{\pi^2 n^2} \\
&\Rightarrow c = \frac{6}{\pi^2} = \frac{c}{n^2}
\end{aligned}$$

Also because

$$\sum_n P((a,b) = n) = 1 = c\left(\frac{1}{1^2} + \frac{1}{2^2} + \dots\right)$$

then $c\frac{\pi^2}{6} = 1 \Rightarrow c = \frac{6}{\pi^2}$ so $P((a,b) = n) = \frac{6}{\pi^2 n^2}$.

If $(a,b) = (c,d)$, they're equal to same n, so

$$\begin{aligned}
P((a,b) = (c,d)) &= \sum_n P((a,b) = n, (c,d) = n) \\
&= \sum_n \frac{1}{\zeta(2)n^2} \frac{1}{\zeta(2)n^2} \\
&= \frac{1}{\zeta(2)^2} \sum_n \frac{1}{n^4} \\
&= \frac{\zeta(4)}{\zeta(2)^2} \\
&= \frac{\frac{\pi^2}{90}}{\left(\frac{\pi^2}{6}\right)^2} \\
&= \frac{2}{5}
\end{aligned}$$

Combinatorial Principles - 1. count in two different ways, 2. pigeon-hole principle, 3. inclusion/exclusion principle

1. Counting in two different ways

Eg.

$$\sum_{d|n} \phi(d) = n$$

by counting set $\{1 \dots n\}$ in 2 different ways.

RHS - count $1, 2, \dots n$.

LHS - split $\{1 \dots n\}$ into subsets dependent on what its gcd with n is.

$$\{1 \dots n\} = \bigsqcup_{d|n} S_d \text{ where } S_d = \{x \in 1 \dots n : (x, n) = d\}$$

If x in S_d then $\frac{x}{d}$ is integer in range $1 \dots \frac{n}{d}$, and also such that $(\frac{x}{d}, \frac{n}{d}) = 1$, conversely if $1 \leq x' \leq \frac{n}{d}$ then $x = x'd$ lies in S_d. So $|S_d|$ is $\phi(\frac{n}{d})$

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

Eg. Binomial Coefficients

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$$

LHS - choose n from $2n$

RHS - choose k from first n and $n-k$ from second n, then use $\binom{n}{n-k} = \binom{n}{k}$ and sum over k from 0 to n

2. Pigeonhole Principle - n pigeonholes and at least $n+1$ pigeons, then some pigeonhole must have at least 2 pigeons

Eg. If p is odd prime, and a, b, c coprime to p, then $ax^2 + by^2 + cz^2 \equiv 0 \mod p$ has a non-trivial solution. Enough to show that $ax^2 + by^2 + c \equiv 0 \mod p$ has a solution (x_0, y_0), since then $(x_0, y_0, 1)$ is solution to original congruence.

Consider the $\frac{p+1}{2}$ integers ax^2, where $x \in \{0, 1, \dots \frac{p-1}{2}\}$. They are all distinct mod p. (If not, then

$$\begin{aligned} ax^2 &\equiv ax'^2 \\ \Rightarrow x^2 &\equiv x'^2 \mod p \\ \Rightarrow x^2 - x'^2 &= (x+x')(x-x') \\ \Rightarrow x' &\equiv \pm x \mod p \end{aligned}$$

but this is impossible if $x \not\equiv x'$ and they're both in range.

Similarly, set of integers $-c - by^2$ as y ranges from 0 to $\frac{p-1}{2}$ are all distinct ($\frac{p+1}{2}$ of them).

So $p+1$ integers in all, but only p residue classes mod p, so there must be two that are congruent mod p, but they can't both be of form ax^2 or of form $-c-by^2$. so we must have some $ax^2 \equiv -c - by^2 \mod p$.

3. Inclusion/Exclusion We'll have a finite set X (universe) and $A, B \subseteq X$.

$$\begin{aligned} |A \cup B| &= |A| + |B| - |A \cap B| \\ |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| \\ &\quad - |B \cap C| + |A \cap B \cap C| \\ \left| \bigcup A_n \right| &= \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_1 < \cdots < i_k \le n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| \\ \left| \overline{\bigcup A_n} \right| &= \left| \bigcap \overline{A_n} \right| = \sum_{k=0}^{n} (-1)^k \sum_{1 \le i_1 < \cdots < i_k \le n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_n}| \end{aligned}$$

where $k = 0$ (empty intersection) is defined to be all of X.

Proof. For any element x of X - if in none of A_i, then it gets counted (on RHS) exactly once in empty intersection, equation to number of times it's counted in LHS. If $x \in X$ is in exactly m of these sets ($m \ge 1$), then it gets counted (choosing k sets from among m sets in which x appears

$$\sum_{k=0}^{n} (-1)^k \binom{m}{k} = \sum_{k=0}^{m} (-1)^k \binom{m}{k} = (1-1)^m = 0$$

this equals contribution to LHS. ■

Another way - let χ_{A_i} be the characteristic function of the set A_i, where

$$\chi_{A_i}(x) = \begin{cases} 1 & x \in A_i \\ 0 & \text{otherwise} \end{cases}$$

The element x is not in any of the A_i when each of $\chi_{A_i}(x) = 0$ - ie., $(1-\chi_{A_i})(x) = 1$

$$\prod_{i=1}^{n}(1-\chi_{A_i})(x) = \begin{cases} 1 & x \notin A_i \forall\, i \\ 0 & \text{otherwise} \end{cases}$$
$$= \chi_{\overline{\bigcup A_i}}$$
$$\text{So } \chi_{\overline{\bigcup A_i}} = (1-\chi_{A_1})(1-\chi_{A_2})\dots$$
$$= 1 - \sum \chi_{A_i} + \sum \underbrace{\chi_{A_i}\chi_{A_j}}_{\chi_{A_i \cap A_j}} \dots$$

Summing $\chi_{\overline{\bigcup A_i}}(x)$ over all $x \Rightarrow$

$$\left|\overline{\bigcup A_i}\right| = |x| - \sum |A_i| + \sum |A_i \cap A_j| \dots$$

Eg. If $n = p_1^{e_1}\dots p_n^{e_n}$, $\phi(n) = n(1-\frac{1}{p_1})\dots(1-\frac{1}{p_n})$. $X = \{1\dots n\}$, $A_i = \{m \in X : p_i | m\}$. If $(m,n) > 1$, then some p_i must divide m and conversely. So $\left|\overline{\bigcup A_i}\right| = \phi(n)$. $|A_i| = \frac{n}{p_i}$, $|A_i \cap A_j| = \frac{n}{p_i p_j}$, etc. So RHS says

$$n - \frac{n}{p_1} - \dots \frac{n}{p_r} + \frac{n}{p_1 p_2} \dots - \frac{n}{p_1 p_2 p_3} \dots$$
$$= n(1 - \frac{1}{p_1} - \dots \frac{1}{p_r} + \frac{1}{p_1 p_2} \dots - \frac{1}{p_1 p_2 p_3} \dots)$$
$$= n \prod \left(1 - \frac{1}{p_i}\right)$$

Recurrences - Recurrence is a rule for generating the next element of a sequence from previous elements.

Eg. $a_0 = 1, a_n = n a_{n-1}$ for $n \geq 1 \Rightarrow a_n = n!$

Eg. $a_0 = 0, a_1 = 1, a_n = a_{n-1} + n \Rightarrow a_n = \frac{n(n+1)}{2}$

Eg. $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$ This is the Fibonacci sequence, where

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

$|(1-\sqrt{5})/2| < 1$, and $|\frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n| < \frac{1}{2}$, so F_n is the closest integer to $\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n$. Implies that $F_{n+1}/F_n \Rightarrow \frac{1+\sqrt{5}}{2}$ as $n \Rightarrow \infty$.

We'll see how to get this explicit formula from the theory of linear of recurrences with constant coefficients (very similar to linear ordinary differential equations with constant coefficients).

Eg. Start with a linear recurrence $u_n + au_{n-1} + bu_{n-2} = 0$ for $n \geq 2$, given initial values. To get explicit formula, we'll use characteristic polynomial $T^n + aT^{n-1} + bT^{n-2} = 0 \Rightarrow T^2 + aT + b = 0$ and use the roots of this characteristic polynomial.