Lecture 17

More on Generating Functions, Two Squares Theorem

Generating Functions - for a sequence $a_0 \dots$ we can define $A(x) = \sum_{a_n \geq 0} a_n x^n$. Eg - if $\{a_n\}$ satisfies a linear recurrence $= a_0 + a_1 x + a_2 x^2 \dots$ then $A(x)$ will be a rational function of x. If we know $A(x)$ then a_n can be obtained as coefficients of x^n in $A(x)$.

1. If $a_n = r^n$ for some fixed r then $A(x) = 1 + rx + r^2x^2 \dots = \frac{1}{1-rx}$.

2. If $A(x)$ is a generating function for $\{a_n\}$ and $B(x)$ for $\{b_n\}$, and α, β are constants, then $\{\alpha a_n + \beta b_n\}$ has generating function $\alpha A(x) + \beta B(x)$.

$$\sum(\alpha a_n + \beta b_n)x^n = \alpha \sum a_n x^n + \beta \sum b_n x^n$$

3. Shift - if $A(x)$ is generating function for $\{a_n\}$, then $xA(x)$ is generating function for sequence $\{a_{n-1}\}$ (ie., $\{0, a_0, a_1, \dots\}$)

4. Generating function for $\{na_n\}$ is $x\frac{dA(x)}{dx}$.

$$\begin{aligned} A(x) &= \sum_{n\geq 0} a_n x^n \\ \frac{dA(x)}{dx} &= \sum_{n \geq 0} n a_n x^{n-1} \\ x\frac{dA(x)}{dx} &= \sum_{n\geq 0} n a_n x^n \end{aligned}$$

Eg.

$$\begin{aligned} \frac{1}{1-x} &= 1 + x + x^2 \dots \\ \frac{1}{(1-x)^2} &= 1 + 2x + 3x^2 \dots \\ \text{so } \frac{x}{(1-x)^2} &= x + 2x^2 + 3x^3 \dots = \sum nx^n \end{aligned}$$

Eg. Generating function for $\{n^2 a_n\}$ is

$$x\frac{d}{dx}\left(x\frac{d}{dx}A(x)\right) = x\frac{dA}{dx} + x^2\frac{d^2A}{dx^2}$$

5.

$$\begin{aligned}
A(x) &= a_0 + a_1x + a_2x^2 \dots \\
B(x) &= b_0 + b_1x + b_2x^2 \dots \\
A(x)B(x) &= (a_0 + a_1x + a_2x^2 \dots)(b_0 + b_1x + b_2x^2 \dots) \\
&= a_0b_0 + (a_1b_0 + b_1a_0)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 \dots \\
&= \text{generating function for } \{c_n\}, \quad c_n = \sum_{k=0}^{n} a_k b_{n-k}
\end{aligned}$$

6. Can be useful, when we want to evaluate partial sums of series (e.g., $\sum\limits_{k\equiv 1 \pmod 7} a_n$). Useful technique - plug in roots of unity.

Eg. We know the generating function for $\{(\frac{1}{2})^n\}$ is $\frac{1}{1-\frac{1}{2}x}$

$$\text{ie., } 1 + \left(\frac{1}{2}\right)x + \left(\frac{1}{2}\right)^2 x^2 \dots = \frac{1}{1-\frac{1}{2}x}$$

$$\begin{aligned}
\sum_{n\equiv 0 \mod 4} \left(\frac{1}{2}\right)^n &= 1 + \left(\frac{1}{2}\right)^4 + \left(\frac{1}{2}\right)^8 \dots \\
&= \frac{1}{1-(\frac{1}{2})^4} = \frac{1}{1-\frac{1}{16}} = \frac{16}{15}
\end{aligned}$$

Another way to see it: plug in 4 roots of unity ($z^4 - 1 = 0, z = \pm 1, \pm i$)

$$\begin{aligned}
1 + \left(\frac{1}{2}\right) + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^3 \dots &= \frac{1}{1-\frac{1}{2}} &&= 2 \text{ (A)} \\
1 + \left(-\frac{1}{2}\right) + \left(-\frac{1}{2}\right)^2 + \left(-\frac{1}{2}\right)^3 \dots &= \frac{1}{1+\frac{1}{2}} &&= \frac{2}{3} \text{ (B)} \\
1 + \left(\frac{1}{2}i\right) + \left(\frac{1}{2}i\right)^2 + \left(\frac{1}{2}i\right)^3 \dots &= \frac{1}{1-\frac{1}{2}i} &&= \frac{2}{2-i} \text{ (C)} \\
1 + \left(-\frac{1}{2}i\right) + \left(-\frac{1}{2}i\right)^2 + \left(-\frac{1}{2}i\right)^3 \dots &= \frac{1}{1+\frac{1}{2}i} &&= \frac{2}{2+i} \text{ (D)}
\end{aligned}$$

Add them, and use the fact that

$$1^n + (-1)^n + (i)^n + (-i)^n = \begin{cases} 0 & n \not\equiv 0 \mod 4 \\ 4 & n \equiv 0 \mod 4 \end{cases}$$

$$
\begin{aligned}
4\left(1+\left(\frac{1}{2}\right)^4+\left(\frac{1}{2}\right)^8\dots\right) &= 2+\frac{2}{3}+\frac{2}{2-i}+\frac{2}{2+i}\\
&= \frac{64}{15}\sum_{n\equiv 0 \mod 4}\left(\frac{1}{2}\right)^n\\
&= \frac{16}{15}
\end{aligned}
$$

Eg. $n \equiv 3 \mod 4$, $a+(\frac{1}{2})\dots xi$

$$
\begin{aligned}
\frac{1}{1^2} &= 1+\left(\frac{1}{2}\right)+\left(\frac{1}{2}\right)^2\dots\\
\frac{1}{i^2} &= 1+\left(\frac{1}{2}i\right)+\left(\frac{1}{2}i\right)^2\dots\\
\frac{1}{(-1)^3} &= -1\left[1+\left(\frac{1}{2}\right)^2+\dots\left(\frac{1}{3}\right)^3\dots\right]
\end{aligned}
$$

If we want to evaluate $\sum_{n\equiv 3 \mod 4}\frac{1}{2^n}$ then multiply (A), (B), (C), (D) by 1^{-3}, $(-1)^{-3}$, i^{-3}, $(-i)^{-3}$ and then add.

7. Zeta functions are very much like geometric functions, so many of the same techniques apply (differentiation is trickier).

Eg. To calculate $S=-1+\frac{1}{4}-\frac{1}{9}+\frac{1}{16}\dots$ This is $Z(f,2)$ when $f(n)=-1$. Two ways of calculating this S.

$$
\begin{aligned}
\zeta(2) &= 1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}\dots\\
&= \frac{\pi^2}{6}\\
\zeta(2)+S &= 2\left(\frac{1}{4}+\frac{1}{16}+\frac{1}{36}\dots\right)\\
&= \frac{1}{2}\left(\frac{1}{1^2}+\frac{1}{2^2}\dots\right)\\
&= \frac{1}{2}\zeta(2)\\
S &= \frac{-\pi^2}{12}
\end{aligned}
$$

or

$$
\begin{aligned}
-S &= 1 - \frac{1}{4} + \frac{1}{9} - \frac{1}{16} \cdots \\
&= \left(1 - \frac{1}{2^2} - \frac{1}{4^2} - \frac{1}{16^2} \cdots\right) \prod_{p \text{ odd}} \left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \cdots\right) \\
\zeta(2) &= \frac{\pi^2}{6} \\
&= \sum \frac{1}{n^2} \\
&= \left(1 + \frac{1}{2^2} + \frac{1}{4^2} + \frac{1}{16^2} \cdots\right) \prod_{p \text{ odd}} \left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \cdots\right)
\end{aligned}
$$

Only differ at the Euler factor at 2:

$$
\begin{aligned}
\frac{(-S)}{\frac{\pi^2}{6}} &= \frac{1 - \frac{1}{2^2} - \frac{1}{4^2} \cdots}{1 + \frac{1}{z^2} + \frac{1}{4z^2} \cdots} \\
&= \frac{1 - \frac{1}{4}\left(\frac{1}{1-\frac{1}{4}}\right)}{\left(-\frac{1}{1-\frac{1}{4}}\right)} \\
&= \frac{1}{2}
\end{aligned}
$$

so $S = -\frac{\pi^2}{12}$.

Theorem 57 (Two Square Theorem)**.** *A prime p is a sum of two integer squares if and only if $p = 2$ or $p \equiv 1 \mod 4$.*

Proof. If $p = 2$ then $2 = 1^2 + 1^2$, so assume p odd from now on. If $p = a^2 + b^2$ then one of a and b must be event and one must be odd, since $\text{odd}^2 \equiv 1 \mod 4$ and $\text{even}^2 \equiv 0 \mod 4 \Rightarrow p \equiv 1 \mod 4$ - ie., condition of being $1 \mod 4$ is necessary.

Reduction: Need to show that any prime $p \equiv 1 \mod 4$ is sum of two squares. We'll show by (strong) induction on p - ie., assume every prime $q < p$ which is $1 \mod 4$ is a sum of two squares.

Lemma 58. *There's a positive integer $< p$ such that $a^2 + m^2 = mp$.*

Proof. 1 is a quadratic residue mod p so there exists some integer x such that $x^2 \equiv -1 \mod p$ (can assume that $|x| < \frac{p}{2}$ because $0, \pm 1, \pm 2 \cdots \pm \frac{p-1}{2}$ is a complete residue system mod p). Therefore $p | x^2 + 1$ and $x^2 + 1 < \frac{p^2}{4} + 1 < p^2$, so $x^2 + 1 = mp$ with $0 < m < p$. $\square$

Let m be the smallest positive integer such that mp is a sum of 2 integer squares. If $m = 1$ we're done with the induction step. If $m > 1$ we'll get a contradiction by constructing a smaller m. Assume $m > 1$. We have $a^2 + b^2 = mp$, so $|a|, |b| < p$ since $a^2, b^2 \leq a^2 + b^2 = mp, p^2$.

First, (a, b) must be 1. Else if $g = (a, b) > 1$ then $(\frac{a}{g})^2 + (\frac{b}{g})^2$ would be a smaller integer multiple of p. (Note: $g < p$ so dividing by g^2 doesn't cancel p).

Next, m must be odd. If not, then $a^2 + b^2$ is even, so a and b have same parity (in fact, both odd since $(a, b) = 1$). Then

$$\left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 = \frac{1}{2}(a^2 + b^2) = \frac{1}{2}mp = \left(\frac{m}{2}\right)p$$

contradicting minimality of m.

Now let q be an odd prime dividing m, let $m = qn$.

$$a^2 + b^2 = mp = qnp \Rightarrow a^2 + b^2 \equiv 0 \mod q$$

Note that $q \nmid a$ and $q \nmid b$ (otherwise q divides both a and b, contradicting $(a, b) = 1$). So

$$\begin{aligned} (ab^{-1})^2 &\equiv -1 \mod q \\ \Rightarrow q &\equiv 1 \mod 4 \end{aligned}$$

By induction hypothesis, $q = c^2 + d^2$ is a sum of two squares.

$$\begin{aligned} a^2 &\equiv -b^2 \mod q \\ c^2 &\equiv -d^2 \mod q \\ (ac)^2 &\equiv (bd)^2 \mod q \\ ac &\equiv \pm bd \mod q \end{aligned}$$

Assume wlog that $ac \equiv bd \mod q$ (if $ac \equiv -bd \mod q$, replace c with $-c$ in $q = c^2 + d^2$). We now have

$$\begin{aligned} a^2 + b^2 &= pqn \\ c^2 + d^2 &= q \\ (a^2 + b^2)(c^2 + d^2) &= pq^2 n \\ (ac - bd)^2 + (ad + bc)^2 &= pq^2 n \quad \text{("miracle of complex numbers")} \end{aligned}$$

Now, we know $q | ac - bd$, so also divides $ad + bc$, so $ad + bc \equiv 0 \mod q$, since

$$\begin{aligned} (ac - bd)^2 + (ad + bc)^2 &\equiv (a^2 + b^2)\underbrace{(c^2 + d^2)}_{q} \\ &\equiv 0 \mod q \end{aligned}$$

so

$$\left(\frac{ac-bd}{q}\right)^2+\left(\frac{ad+bc}{q}\right)^2=pn$$

So we replaced m by n which is $< m$, resulting in contradiction. ($\lightning$) $\blacksquare$