Friday June 5th, 10:00AM - 11:30AM

Stefan Cohn-Vossen room

Some Applications of Modular Forms in Number Theory

Def A *partition* of a non-negative integer n is a weakly decreasing sequence of positive integers that sums to n. The number of partitions of n is denoted by $p(n)$.

Ex $p(0) = 1$ $\quad$ empty partition

$p(1) = 1$ $\quad$ (1)

$p(2) = 2$ $\quad$ (2), $(1,1)$

$p(3) = 3$ $\quad$ (3), $(2,1)$, $(1,1,1)$

$p(4) = 5$

(4), $(3,1,1)$, $(2,2)$, $(2,1,1)$, $(1,1,1,1)$

$p(5) = 7$

(5), $(4,1)$, $(3,2)$, $(3,1,1)$, $(2,2,1)$, $(2,1,1,1)$, $(1,1,1,1,1)$

Since the condition of the sequence says order does not matter, partitions are instead often written additively:

$3+1+1$ instead of $(3,1,1)$.

What is the connection to modular forms?

<u>Theorem</u> The generating function for $p(n)$ is given by, for $|q|<1$,

$$\sum_{n=0}^{\infty} p(n) q^n = \prod_{n=1}^{\infty} \frac{1}{1-q^n} = q^{1/24}/\eta(\tau)$$

where $q = e^{2\pi i \tau}$ and $\eta(\tau)$ is Dedekind's eta-function (a weight 1/2 weakly holomorphic modular form with multiplier).

$\boxed{\text{proof}}$

By expanding as geometric series, we have

$$\frac{1}{1-q} = 1 + q + q^2 + q^3 + q^4 + \cdots,$$

$$\frac{1}{1-q^2} = 1 + q^{1\cdot 2} + q^{2\cdot 2} + q^{3\cdot 2} + q^{4\cdot 2} + \cdots,$$

$$\frac{1}{1-q^3} = 1 + q^{1\cdot 3} + q^{2\cdot 3} + q^{3\cdot 3} + q^{4\cdot 3} + \cdots,$$

$$\frac{1}{1-q^n} = 1 + q^{1\cdot n} + q^{2\cdot n} + q^{3\cdot n} + q^{4\cdot n} + \cdots$$

To be careful about convergence, we will first show that

$$\sum_{n=0}^{\infty} p_M(n) q^n = \prod_{n=1}^{M} \frac{1}{1-q^n}, \qquad (A)$$

where $p_M(n)$ is the number of partitions of n with all parts at most M.

Any partition is uniquely determined by how many times 1 appears as a part, how many times 2 appears as a part, how many times 3 appears as a part, and so on. Thus

$$\sum_{n=0}^{\infty} p_M(n) q^n = (1+q+q^2+q^3+\cdots)$$
$$* (1+q^{1\cdot 2}+q^{2\cdot 2}+q^{3\cdot 2}+\cdots)$$
$$* (1+q^{1\cdot 3}+q^{2\cdot 3}+q^{3\cdot 3}+\cdots)$$
$$* \cdots$$
$$* (1+q^{1\cdot M}+q^{2\cdot M}+q^{3\cdot M}+\cdots)$$
$$= \frac{1}{1-q} * \frac{1}{1-q^2} * \frac{1}{1-q^3} * \cdots * \frac{1}{1-q^M},$$

which proves ⊛.

By definition
$$\lim_{M\to\infty} \prod_{n=1}^{M} \frac{1}{1-q^n} = \prod_{n=1}^{\infty} \frac{1}{1-q^n}.$$

For fixed n, $\lim_{M\to\infty} p_M(n) = p(n)$, since
$p(n) = p_M(n)$ for $M \geq n$. We must justify the exchange of limits
$$\lim_{M\to\infty} \sum_{n=0}^{\infty} p_M(n) q^n = \sum_{n=0}^{\infty} \lim_{M\to\infty} p_M(n) q^n$$

First we suppose $0 \leq q < 1$, so that $0 \leq p_M(n) q^n \leq p(n) q^n$, and so by the

Monotone Convergence Theorem,

$$\lim_{M\to\infty} \sum_{n=0}^{\infty} p_M(n)q^n = \sum_{n=0}^{\infty} p(n)q^n.$$

Thus ⊛ holds for $0 \le q < 1$.
This implies the LHS of ⊛ has radius of convergence 1, and so both the LHS and RHS are holomorphic functions for $|q|<1$. By the identity theorem of complex analysis, ⊛ holds for $|q|<1$.

$\square$

Convergence issues usually work out exactly as in the above proof, so they are usually ignored. To say a little bit about infinite products,

- given a sequence of complex numbers $\{a_n\}_{n=1}^{\infty}$, the product $\prod_{n=1}^{\infty} a_n$ converges if

  $\lim_{M\to\infty} \prod_{n=1}^{M} a_n$ exists and is non-zero.

  Product diverge to zero.

- $\prod_{n=1}^{\infty}(1+a_n)$ converges if & only if $\sum_{n=1}^{\infty} a_n$ converges

- The product $\prod_{n=1}^{\infty}(1+a_n)$ is said to converge absolutely if $\prod_{n=1}^{\infty}(1+|a_n|)$ converges.

- When a product converges absolutely reordering of terms is allowed.

This means rearrangements like the following are valid: for $|q|<1$

$$\prod_{n=1}^{\infty}\frac{1}{1-q^n} = \frac{1}{\prod_{n=1}(1-q^n)}$$

$$= \frac{1}{\prod_{n=1}^{\infty}(1-q^{2n-1})(1-q^{2n})}$$

$$= \frac{1}{\left[\prod_{n=1}^{\infty}(1-q^{2n-1})\right]*\left[\prod_{n=1}^{\infty}(1-q^{2n})\right]}.$$

The first product converges since

$$\frac{1}{1-q^n} = 1+\frac{q^n}{1-q^n}.$$

<u>Theorem</u> (Ramanujan) For $n\geq 0$,

$p(5n+4)\equiv 0 \pmod 5$,

$p(7n+5)\equiv 0 \pmod 7$, and

$p(11n+6)\equiv 0 \pmod{11}$.

The proof will use Sturm's Theorem, which is as follows:

Suppose $f(\tau) = \sum_{n=0}^{\infty} a(n) q^n \in \mathbb{Z}[[q]]$ and f is a holomorphic modular form of weight k (with $k \in \frac{1}{2}\mathbb{Z}$) on $\Gamma_0(N)$ with Dirichlet character χ. Let m be a positive integer.

If $m \mid a(n)$ for $0 \le n \le B$, where
$$B = \frac{k}{12} \cdot [SL_2(\mathbb{Z}) : \Gamma_0(N)],$$
then $m \mid a(n)$ for all n.

$\boxed{\text{proof of congruences}}$

Suppose ℓ is prime. Since reduction mod ℓ is a ring homomorphism from $\mathbb{Z}[[q]]$ to $\mathbb{Z}/\ell\mathbb{Z}[[q]]$ and $\mathbb{Z}/\ell\mathbb{Z}[[q]]$ has characteristic ℓ, we have

$$\prod_{n=1}^{\infty} (1-q^n)^{\ell} \equiv \prod_{n=1}^{\infty} (1-q^{\ell n}) \pmod{\ell}.$$

Here the congruence is in $\mathbb{Z}[[q]]$.

Set $F_\ell(q) = \sum_{n=0}^{\infty} f_\ell(n) q^n = \prod_{n=1}^{\infty} (1-q^{\ell n})^\ell \sum_{n=0}^{\infty} p(n) q^n$.

We see that $p(\ell n + r) \equiv 0 \pmod{\ell}$ for all n if and only if $f_\ell(\ell n + r) \equiv 0 \pmod{\ell}$ for all n. Why?

Write

$$\sum_{n=0}^{\infty} p(n) q^n = \sum_{k=0}^{\ell-1} q^k * A_k(q^\ell),$$

$$F_\ell(q) = \sum_{k=0}^{\ell-1} q^k * B_k(q^\ell),$$

with $A_k(q), B_k(q) \in \mathbb{Z}[[q]]$.

Note

$$B_k(q) = \prod_{n=1}^{\infty} (1-q^{\ell n})^\ell * A_k(q),$$

and

$$p(\ell n + r) \equiv 0 \pmod{\ell} \quad \text{for all } n$$

if and only if

$$A_r(q^\ell) = 0 \quad \text{in } (\mathbb{Z}/\ell\mathbb{Z})[[q]]$$

if & only if

$$B_r(q^\ell) = 0 \quad \text{in } (\mathbb{Z}/\ell\mathbb{Z})[[q]]$$

(since $\prod_{n=1}^{\infty} (1-q^{\ell n})^\ell$ is invertible)

if & only if

$$f_\ell(\ell n + r) \equiv 0 \pmod{\ell} \quad \text{for all } n.$$

Note $F_\ell(q) = q^{\frac{1-\ell^2}{24}} \cdot \frac{\eta(\ell\tau)^\ell}{\eta(\tau)}$,

and

$\eta(\ell\tau)^\ell/\eta(\tau)$ is a weight $\left(\frac{\ell-1}{2}\right)$ holomorphic modular form on $\Gamma_0(\ell)$, with multiplier, for $\ell \geq 5$ prime.

Set $G_\ell(q) = \frac{\eta(\ell\tau)^\ell}{\eta(\tau)} = \sum_{n=0}^{\infty} g_\ell(n) q^n$.

Note $\frac{\ell^2-1}{24}$ is an integer for ℓ prime with $\ell \geq 5$,

in particular,

ℓ	$(\ell^2-1)/24$
5	$1 \equiv -4 \pmod 5$
7	$2 \equiv -5 \pmod 7$
11	$5 \equiv -6 \pmod{11}$

Thus the three partition congruences are equivalent to $g_\ell(\ell n) \equiv 0 \pmod \ell$ for $\ell = 5, 7$, and 11. This is equivalent to $U_\ell(g_\ell(\tau)) \equiv 0 \pmod \ell$, where U_ℓ is Atkin's U-operator

$U_\ell : M_k(\Gamma_0(\ell), \chi) \to M_k(\Gamma_0(\ell), \chi)$,

$$\sum_{n\geq 0} a(n)q^n \mapsto \sum_{n\geq 0} a(\ell n)q^n.$$

The bounds B in Sturm's theorem for $M_2(\Gamma_0(5),\chi)$, $M_3(\Gamma_0(7),\chi)$, and $M_5(\Gamma_0(11),\chi)$ are 1, 2, and 5.

We can instead check
$p(5n+4)\equiv 0 \pmod 5$ for $0\leq n\leq 1$,
$p(7n+5)\equiv 0 \pmod 7$ for $0\leq n\leq 2$, and
$p(11n+6)\equiv 0 \pmod 7$ for $0\leq n\leq 5$.

n	$p(5n+4)$	$p(7n+5)$	$p(11n+6)$
0	5	7	11
1	30	77	297
2	135	490	3718
3	490	2436	31185
4	1575	10143	204226
5	4565	37338	1121505
6	12310	124754	5392783

$\square$

Modular forms can also be used for deducing asymptotics. There is not time for the proof.

Theorem (Hardy-Ramanujan-Rademacher)
We have

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} A_k(n)\sqrt{k}\, \frac{d}{dn} \frac{\sinh\left(\frac{\pi}{k}\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)}\right)}{\sqrt{n-1/24}}$$

in particular,

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}$$

Many other counting functions also match up with modular forms. Some are even simpler.

Def A composition of a non-negative integer is a sequence of positive integers that sums to n.

Proposition The number of compositions of n is 2^{n-1}.

proof
Each composition of n is built as $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ from

(1 plus or comma 1 plus or comma 1 ... plus or comma 1).

So 2 choices $n-1$ times. □