Seminar Notes 02/14/05

Subject Matter: *On rational values of* $\phi(n!)/m!$ *and* $\sigma(n!)/m!$

Joint Work With: Dan Baczkowski and Ognian Trifonov

Notations: N is a positive integer
p and q are primes
$\Phi_N(x)$ is the Nth cyclotomic polynomial (define; note some values)

Properties of Cyclotomic polynomials:

$$\Phi_{pN}(x) = \begin{cases} \Phi_N(x^p) & \text{if } p|N \\ \Phi_N(x^p)/\Phi_N(x) & \text{if } p \nmid N \end{cases} \qquad\qquad x^N - 1 = \prod_{d|N} \Phi_d(x)$$

Lemma 4: *Let q be a prime, and let a and N be integers with $N \geq 1$. Write $N = q^r M$ where r and M are integers with $r \geq 0$ and $q \nmid M$. Then $q|\Phi_N(a)$ if and only if $M = \mathrm{ord}_q(a)$. Also, if $r \geq 1$ and $N > 2$, then $q^2 \nmid \Phi_N(a)$.*

Proof:

- $\boxed{\bullet}$ Let $s = \mathrm{ord}_p(a)$, and consider first $M = s$.
  - $\displaystyle\prod_{d|M} \Phi_d(a) \equiv a^M - 1 \equiv 0 \pmod{q} \implies q|\Phi_M(a)$.
  - Use $\Phi_N(x) \equiv \Phi_M(x)^{q^{r-1}(q-1)} \pmod{q}$ and set $x = a$.
- $\boxed{\bullet}$ Assume $q|\Phi_N(a)$ and $M \neq s$.
  - $a^M \equiv a^N \equiv 1 \pmod{q} \implies a \not\equiv 0 \pmod{q}$, $s|M$ and, hence, $s < M$.
  - Therefore, $(x^s - 1)\Phi_M(x)$ is a factor of $x^M - 1$.
  - Note that $x - a$ is a factor of each of $x^s - 1$ and $\Phi_M(x)$ modulo q.
  - Thus, $x^M - 1 \equiv (x-a)^2 g(x) \pmod{q}$ for some $g(x) \in \mathbb{Z}[x]$. Take derivatives and set $x = a$.
- $\boxed{\bullet}$ $\Phi_N(x)$ is a factor of $\dfrac{(x^{N/q})^q - 1}{x^{N/q} - 1} = (x^{N/q})^{q-1} + (x^{N/q})^{q-2} + \cdots + (x^{N/q})^2 + x^{N/q} + 1.$
  - Substitute $x = a$ on the left. If $q|\Phi_N(a)$, then $a^{N/q} \equiv 1 \pmod{q}$.
  - On the right, replace $x^{N/q}$ with $a^{N/q} = kq + 1$, where $k \in \mathbb{Z}$. Deduce that if $q \neq 2$, then $q^2 \nmid \Phi_N(a)$.
- $\boxed{\bullet}$ $\Phi_N(1) = p$ if N is a power of a prime p and $\Phi_N(1) = 1$ if N is an integer with more than one distinct prime factor.
  - Also, $N > 1$ implies $\Phi_N(0) = 1$. Hence, $\Phi_N(a) \equiv 1 \pmod{2}$ if N is not a power of 2 or if a is even.
  - For $N = 2^r$ with $r \geq 2$ and a odd, use $\Phi_N(a) \equiv \Phi_{2^r}(a) \equiv a^{2^{r-1}} + 1 \equiv 2 \pmod{4}$.

Corollary 2: *Let q be a prime, and let a and N be integers with $N > 2$. If $q|\Phi_N(a)$, then either $q \equiv 1 \pmod{N}$ or we have that both q is the largest prime factor of N and $q^2 \nmid \Phi_N(a)$.*

Lemma 5: *Let q be an odd prime, and let r and ℓ be positive integers. Let $f(x) = x^\ell + x^{\ell-1} + \cdots + x + 1$. Then $f(x)$ has $\le \ell$ distinct roots modulo q^r.*

Proof:

- Let $n = \ell + 1$ and note $(x-1)f(x) = x^n - 1$. Thus, $f(a) \equiv 0 \pmod{q^r}$ implies $a^n \equiv 1 \pmod{q^r}$ (and $q \nmid a$).
- Let g be a primitive root modulo q^r, and set $d = \gcd\big(n, \phi(q^r)\big) = \gcd\big(n, q^{r-1}(q-1)\big)$.
- Let s be the integer in $\{1, 2, \dots, \phi(q^r)\}$ for which $a \equiv g^s \pmod{q^r}$, so $g^{ns} \equiv a^n \equiv 1 \pmod{q^r}$.
- Note $g^{ns} \equiv 1 \pmod{q^r}$ if and only if s is a multiple of $\phi(q^r)/d$,.
- There are exactly d incongruent integers a modulo q^r for which $a^n \equiv 1 \pmod{q^r}$. Done if $n \nmid \phi(q^r)$.
- If $n|\phi(q^r)$, use $f(1) = \ell + 1 = n \le (q-1)q^{r-1} < q^r$.

Lemma 6: *Let k be a positive integer. There are positive numbers c_k and n_k such that if $n \ge n_k$, then either n has $\ge k+1$ prime factors that are $\le \log n/(\log\log n)^2$ or $\phi(n) \ge c_k n$.*

Proof:

- Recall $\displaystyle\prod_{p \le z} \left(1 - \frac{1}{p}\right) \sim \frac{A}{\log z}$.
- Suppose n is large and that n has $\le k$ prime factors that are $\le \log n/(\log\log n)^2$.
- $\displaystyle\left(\frac{\log n}{(\log\log n)^2}\right)^{2\log n/\log\log n} > n$.
- Hence, there are $< 2\log n/\log\log n$ primes $> \log n/(\log\log n)^2$ that divide n.
- Deduce from $\pi(3\log n) > 2\log n/\log\log n$ that $\phi(n) \ge c_k n$.

Lemma 7: *Let a and b be positive relatively prime integers, and let $I \subset [0, \infty)$ be an interval of length $h > b$. Then the number of primes in I that are $\equiv a \pmod{b}$ is*

$$\le 2h/\big(\phi(b)\log(h/b)\big).$$

Lemma 8: *Fix primes q_1 and q_2 and a number $\varepsilon > 0$. Let n_1 and n_2 be sufficiently large integers. Then*

$$\gcd\left(q_1^{n_1} - 1, q_2^{n_2} - 1\right) < \max\{q_1^{\varepsilon n_1}, q_2^{\varepsilon n_2}\}.$$