Number Theory Section Summary: 5.3
Fermat's Little Theorem

1. Summary

The most important result in this section is "Fermat's Little Theorem". This is one of the crucial results which has made number theory so valuable in recent years (in cryptography). Number theory was beloved of Hardy because he thought it practically useless - how wrong could he be!

2. Definitions

pseudoprime: a composite number n such that $n|2^n - 2$.

A Chinese theorem of 2500 years ago speculated that numbers that so divide are prime, and that primes so divide. It was proven wrong by counterexample (341), in 1819.

pseudoprime to the base a: more generally, a composite number n such that $n|a^n - a$.

absolute pseudoprime: a composite number n which satisfies $a^n \equiv a(\text{mod n})$ for all integers a.

3. Theorems

Theorem 5.1 (Fermat's Theorem): Let p be prime and suppose that p does not divide a. Then $a^{p-1} \equiv 1(\text{mod p})$.

Corollary: If p is a prime, then $a^p \equiv a(\text{mod p})$ for any integer a.

The corollary is a generalization of Fermat's little theorem, which obviates the need to include the divisibility criterion. At times, though,

it's really Fermat's little theorem that one wants to use, since it's nice to get large powers to work out to 1....

The proof of the corollary by induction is really interesting! It's surprising that induction would work here, perhaps – at least, it surprised me.

The rest of the section deals with numbers that have primal pretentions: pseudoprimes, and pseudoprimes to a base a, and absolute pseudoprimes.

Lemma: If p and q are distinct primes with $a^p \equiv a (\text{mod q})$ and $a^q \equiv a (\text{mod p})$, then $a^{pq} \equiv a (\text{mod pq})$.

Theorem 5.2: If n is an odd pseudoprime, then $M_n = 2^n - 1$ is a larger one.

Theorem 5.3: Let n be a composite square-free integer, say, $n = p_1 p_2 \cdots p_r$, where the p_i are distinct primes. If $p_i - 1 | n - 1$ for $i = 1, 2, \ldots, r$, then n is an absolute pseudoprime.

4. Properties/Tricks/Hints/Etc.

So absolute pseudoprimes behave like primes, as far as Fermat's Little theorem is concerned. Fermat's little theorem couldn't detect them as pretenders.

To prove: For prime p,

$a^p \equiv a \pmod{p}$ $\forall a \in \mathbb{N}$

By induction.

Base case: $a = 1$.

$1^p \equiv 1 \pmod{p}$ ✓

Inductive Step: Consider the statement

true for $a = k$; show that it is true for $k+1$.

Assume $k^p \equiv k \pmod p$

Consider

$$(k+1)^p = k^p + \binom{p}{1} k^{p-1} \cdot 1 + \binom{p}{2} k^{p-2} \cdot 1^2 + \dots + \binom{p}{p-2} k^2 \cdot 1^{p-2} + \binom{p}{p-1} k \cdot 1^{p-1} + 1 \quad (5)$$

Lemma: $p \mid \binom{p}{j}$ $\forall j$ $1 \le j \le p-1$

$$\binom{p}{j} = \frac{p!}{j!(p-j)!} = \frac{p(p-1)\cdots(p-j+1)}{j!}$$

Observe that

$$j! \binom{p}{j} = p(p-1)\cdots(p-j+1) \equiv 0 \pmod p$$

[p. 68 $ab \equiv 0 \pmod p \Rightarrow a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$]

$p \nmid j!$, since $j < p$ & p is prime.

Hence $\binom{p}{j} \equiv 0 \pmod p$. ✓

So by the lemma, (5) yields

$$(k+1)^p \equiv k^p + 1 \equiv k+1 \pmod p$$ ✓

Concluding the proof by induction.

#3 for $n \geq 0$, $13 \mid 11^{12n+6} + 1$

To show $\begin{cases} 11^{12n+6} + 1 \equiv 0 \pmod{13} \\ 11^{12n+6} \equiv -1 \pmod{13} \end{cases}$

$$11^{12n+6} = 11^{12n} \cdot 11^6 \equiv (11^{12})^n \cdot 11^6 \pmod{13}$$

$$\equiv 11^6 \pmod{13} \quad \equiv (-2)^6 \pmod{13}$$

$$\equiv (11^2)^3 \pmod{13} \quad \equiv 64 \pmod{13}$$

$$\equiv (4)^3 \pmod{13}$$

$$\equiv 12 \pmod{13}$$

$$\equiv -1 \pmod{13}$$ ✓

2a. $\gcd(a, 35) = 1$ show that $a^{12} \equiv 1 \pmod{35}$

hint: $a^6 \equiv 1 \pmod{7}$, $a^4 \equiv 1 \pmod{5}$ $\Rightarrow$ $a^{12} \equiv 1 \pmod{7}$, $a^{12} \equiv (a^4)^3 \equiv 1 \pmod{5}$

Consider

$c \equiv d \bmod p$, $c \equiv d \bmod q$, $p \neq q$ $\Rightarrow$

$c = d + ip$, $c = d + jq$ $\Rightarrow$ $ip = jq$

$\therefore q \mid ip$ and $p \mid jq$

$\therefore q \mid i$, so $i = eq$

$c = d + eqp \Rightarrow \boxed{c \equiv d \pmod{pq}}$

Therefore, $a^{12} \equiv 1 \pmod{35}$

#4. $a^7 \equiv a \pmod{42}$ for all a.

$a^7 \equiv a \pmod{7}$

$a^3 \equiv a \pmod{3}$

$a^2 \equiv a \pmod{2}$

$a^7 = a \cdot (a^3)^2 \equiv a \cdot a^2 = a^3 \equiv a \pmod{3}$

$a^7 = a \cdot (a^2)^3 \equiv a \cdot a^3 \equiv a^4 = (a^2)^2 \equiv a^2 \equiv a \pmod{2}$

Conclude that

$a^7 \equiv a \pmod{42}$

#5 $\gcd(a, 30) = 1$ Show that $60 \mid a^4 + 59$

i.e. $a^4 \equiv -59 \equiv 1 \pmod{60}$

$60 = 6 \cdot 10 = 2^2 \cdot 3 \cdot 5$

$a \equiv 1 \pmod{2} \Rightarrow a^4 \equiv 1 \pmod{2}$

$a^2 \equiv 1 \pmod{3} \Rightarrow a^4 \equiv 1 \pmod{3}$

$a^4 \equiv 1 \pmod{5}$

$a^2 \equiv 1 \pmod{8} \Longrightarrow a^2 \equiv 1 \pmod{4}$

$\therefore a^4 \equiv 1 \pmod{4}$

4, 3, + 5 are mutually relatively prime,

so $a^4 \equiv 1 \pmod{4 \cdot 3 \cdot 5} \equiv 1 \pmod{60}$