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. **Theorems**

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

Proof: Consider $\{a, 2a, 3a, \ldots, (p-1)a\}$.

Claim: $ra \not\equiv sa \pmod{p}$ $\forall r, s \in \{1, \ldots, p-1\}$, $r \neq s$

~~By contradiction~~, Assume $ra \equiv sa \pmod{p}$. Then

$\therefore r \equiv s \pmod{p}$.

Then $r = s$. $\therefore rs \not\equiv sa$ if $r \neq s$.

$\therefore$, $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv$

$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p}$

$\therefore$, $a^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}$

$a^{p-1} (p-1)! \equiv (p-1)! \pmod{p}$

$\therefore$, $a^{p-1} \equiv 1 \pmod{p}$ because $\gcd((p-1)!, p) = 1$.

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

Example#2c, p. 96: If $\gcd(133,a) = \gcd(133,b) = 1$

show that $133 \mid a^{18} - b^{18}$

$a^{18} \equiv b^{18} \pmod{133}$

$133 = 7 \cdot 19$

$a^{18} \equiv 1 \pmod{19} \equiv b^{18} \Rightarrow a^{18} \equiv b^{18} \pmod{19}$

$a^{18} - b^{18} = m \cdot 19$

$a^6 \equiv 1 \pmod 7 \equiv b^6$

$\therefore (a^6)^3 \equiv 1 \pmod 7 \equiv (b^6)^3 \Rightarrow a^{18} \equiv b^{18} \pmod 7$

$a^{18} - b^{18} = n \cdot 7$

$\therefore m \cdot 19 = n \cdot 7 \quad \therefore 7 \mid m$, and $19 \mid n$.

$\therefore a^{18} - b^{18} = \underbrace{\frac{m}{7}}_{\in \mathbb{Z}} \cdot 7 \cdot 19 = k \cdot 133 \quad \therefore a^{18} \equiv b^{18} \pmod{133}$

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....

If $r \equiv s \pmod p$ and $r \equiv s \pmod q$ then $r \equiv s \pmod{pq}$

q, p prime

4.2, #13 p69

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

$42 = 2 \cdot 3 \cdot 7$ ●

$a^2 \equiv a \pmod 2$ ✓

$a^3 \equiv a \pmod 3$

$a^7 \equiv a \pmod 7$

$a^7 \pmod 2 \equiv a^2 \cdot a^2 \cdot a^2 a \equiv a^4 \pmod 2 \equiv (a^2)^2 \pmod 2$

$\equiv a^2 \pmod 2 \equiv a \pmod 2$ ✓

$a^7 \pmod 3 \equiv (a^3)^2 \cdot a \equiv a^2 \cdot a \equiv a^3 \equiv a \pmod 3$ ✓

$\therefore\ a^7 \equiv a \pmod{2\cdot 3\cdot 7} \equiv a \pmod{42}$

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

#5. $\gcd(a,30) = 1$ Show that

$60 \mid a^4 + 59$

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

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

$a^4 \equiv 1 \pmod 5$

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

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

Is $a^4 \equiv 1 \pmod 4$? Since a is odd, we know that

$a^2 = 8k+1 \Rightarrow a^2 \equiv 1 \pmod 8$

$= 4(2k)+1 \Rightarrow a^2 \equiv 1 \pmod 4 \Rightarrow a^4 \equiv 1 \pmod 4$

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

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 $a^{pq} \equiv a(\text{mod pq})$.

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

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 ($341|2^{341} - 2$).

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.

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.

3. 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.

Here's #8 in all its glory, without prior simplification to the smallest set of consistent equations.

① $x \equiv 1 \pmod 2$
② $x \equiv 2 \pmod 3$
③ $x \equiv 3 \pmod 4$
④ $x \equiv 4 \pmod 5$
⑤ $x \equiv 5 \pmod 6$
⑥ $x \equiv 0 \pmod 7$

The first equation yields

$x = 2k+1 \equiv 2 \pmod 3$

$\therefore 2k \equiv 1 \pmod 3 \equiv 4$

$k \equiv 2 \pmod 3$

$x = 2(2+3l) + 1$

● $= 5 + 6l \equiv 3 \pmod 4$

Note: equation ⑤ is covered here, so we would know not to pursue it further.

$\therefore 6l \equiv -2 \pmod 4$, or

$2l \equiv -2 \pmod 4$, so

$l \equiv -1 \pmod 2 \equiv 1 \pmod 2$

Here's the mistake you'll make if you're not careful, which will "lose" some solutions.

$x = 5 + 6(1 + 2m)$

$= 11 + 12m$

$x = 11 + 12m \equiv 4 \pmod 5$

$\therefore\ 12m \equiv 2m \equiv 8 \pmod 5$

$m \equiv 4 \pmod 5$

$x = 11 + 12(4 + 5n)$

$= 59 + 60n \equiv 5 \pmod 6$ ← unnecessary if we picked up on the earlier hint...

$\therefore\ 60n \equiv 6 \pmod n$, or $0 \equiv 0 \pmod n$; i.e., there's no additional constraint imposed by this equation.

$x = 59 + 60n \equiv 0 \pmod 7$

$\therefore\ 60n \equiv 4 \pmod 7$

$4n \equiv 4 \pmod 7 \quad \Rightarrow \quad n \equiv 1 \pmod 7$

$\therefore\ x = 59 + 60(1 + 7s)$

$= 119 + 420s$, or

$$\boxed{x \equiv 119 \pmod{420}}$$

119 eggs.

So we could have cut down on our effort a little, by making a few observations, but we ended up getting the right answer. We need to be cautious when cancelling common factors or we might miss some solutions.

If we keep our eyes open, we can see that some equations aren't necessary (e.g. eq ⑤, which imposed no additional constraint).