Chapter 6 Lecture Notes

Greg Knapp

February 27, 2022

1 Wilson's Theorem and Fermat's Little Theorem

1.1 Intro

- Our goal is to get to quadratic reciprocity as soon as we can.
- Quadratic reciprocity essentially describes how to take square roots in modular arithmetic
- To get there, we need a couple of special congruences that we're going to try to prove

1.2 Wilson's Theorem

- In one of our infinitely many primes proofs earlier, we were looking at numbers of the form $n! + 1$
- We said they have to have a prime factor $> n$ and we used that to say something like "since there's a prime $> n$ for each n, there must be infinitely many primes"
- We didn't talk about what prime factors those numbers have though.
- Let's look at some selected examples
- $1! + 1 = 2$ is div by 2
- $2! + 1 = 3$ is div by 3
- $4! + 1 = 25$ is div by 5
- $6! + 1 = 721$ is div by 7
- Note that $3! + 1 = 7$ is not div by 4 and $5! + 1 = 121$ is not div by 6
- So it seems like when p is prime, $(p - 1)! + 1$ is div by p
- **Thm:** (Wilson): If p is prime, then $(p - 1)! \equiv -1 \mod p$
- Proof:
  - $p = 2$ is trivial, so assume p odd
  - $(p - 1)! = (p - 1)(p - 2) \cdots 2 \cdot 1$
  - Note that $p - 1 \equiv -1$ is its own inverse mod p
  - Hence, if $x < p - 1$, then the inverse of x is also $< p - 1$
  - Inverses come in distinct pairs: you saw this on the homework. If x is its own inverse, then $x^2 \equiv 1 \mod p$ implying that $x \equiv \pm 1 \mod p$
  - So the numbers $(p-2), \ldots, 2$ (of which there are $p-3$, i.e. evenly many) can be paired with their inverses and you get a bunch of canceling
  - Hence, $(p - 1)! \equiv p - 1 \equiv -1 \mod p$

- Fact: the converse is also true, though we won't prove it
- If $n \geqslant 2$ has $(n-1)! \equiv -1 \mod n$, then n is prime.
- This can be used as a primality test, though an inefficient one since $n!$ takes a while to compute

1.3 Fermat's Little Theorem

- Something else you noticed on a previous homework: if $a \in \mathbb{Z}$, then $3 \mid a^3 - a$
- Also $5 \mid a^5 - a$
- Easy enough to check that $2 \mid a^2 - a$
- Note that $4 \nmid a^4 - a$ if $a = 2$, so it is not always the case that $a^n - a$ is divisible by n
- But it sure looks like if p is prime, then $p \mid a^p - a$
- **Thm:** (Fermat?) If p is prime and a is an integer with $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$
- Corollary: If $a \in \mathbb{Z}$, then $a^p - a$ is div by p (check both cases)
- Proof:
  - Consider the numbers of the form $a, 2a, 3a, \ldots, (p-1)a$
  - Note that none are divisible by p
  - Note that they are pairwise incongruent mod p
  - Hence, $\{0, a, 2a, \ldots, (p-1)a\}$ forms a complete set of residues mod p
  - Now we have

$$\begin{aligned} a \cdot 2a \cdot 3a \cdots (p-1)a &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p \\ a^{p-1}(p-1)! &\equiv (p-1)! \mod p \\ a^{p-1} &\equiv 1 \mod p \end{aligned}$$

Applications and Examples

- If p is prime and $a \in \mathbb{Z}$, $p \nmid a$, then a^{p-2} is an inverse of $a \mod p$
- **Ex:** What is the remainder when 40! is divided by $41 \cdot 43 = 1763$?
  - Here, we're going to use Sun-Tsu's Theorem in kind of a clever way
  - First, we note that $40! \equiv -1 \mod 41$ by Wilson's Theorem
  - Next, $42! \equiv -1 \mod 43$ also by Wilson's Theorem
  - To get to 40!, we want to multiply by 42^{-1} and 41^{-1}
  - 42^{-1} is itself (-1) and since $41 \equiv -2 \mod 43$, we see that -22 is an inverse to 41 mod 43.
  - Hence, $40! \equiv 42! \cdot 42^{-1} \cdot 41^{-1} \equiv (-1) \cdot (-1) \cdot (-22) \equiv -22 \mod 43$.
  - Now we want to find an integer that is equivalent to $-1 \mod 41$ and $-22 \mod 43$
  - Apply Sun-Tsu's theorem to get $x \equiv 1311 \mod 1763$
- **Ex:** Show that $30 \mid n^9 - n$ for all positive integers n
  - $30 = 2 \cdot 3 \cdot 5$, so we want to look at $n^9 - n$ mod 2, 3, and 5 separately
  - mod 2, we note that $0^9 - 0 \equiv 0 \mod 2$ and $1^9 - 1 \equiv 0 \mod 2$, so $n^9 - n$ is always divisible by 2
  - mod 3, we note that $n^9 - n = (n^3)^3 - n \equiv n^3 - n \equiv 0 \mod 3$

- mod 5, we note that $n^9 - n = n^5 \cdot n^4 - n \equiv n \cdot n^4 - n \equiv n^5 - n \equiv 0 \mod 5$
- Hence, $n^9 - n \equiv 0$ mod 2, 3, and 5 so by Sun-Tsu's Theorem, it is also congruent to 0 mod 30.

- **Ex:** Compute the least positive residue of $3^{201} \mod 11$
  - Since $3^{10} \equiv 1 \mod 11$, we have $3^{201} = 3^{200} \cdot 3 \equiv (3^{10})^{20} \cdot 3 \equiv 3 \mod 11$
- **Ex:** Compute the least positive residue of $5^{4328} \mod 101$
  - We know that $5^{100} \equiv 1 \mod 101$, so $5^{4328} \equiv 5^{28} \mod 101$
  - Still hard to compute, but watch this:

$$\begin{aligned}
5^2 &\equiv 25 \mod 101 \\
5^4 &\equiv 25^2 \equiv 625 \equiv 19 \mod 101 \\
5^8 &\equiv 19^2 \equiv 361 \equiv 58 \mod 101 \\
5^{16} &\equiv 58^2 \equiv 3364 \equiv 31 \mod 101 \\
5^{28} &\equiv 5^{16} \cdot 5^8 \cdot 5^4 \equiv 31 \cdot 58 \cdot 19 \equiv 24 \mod 101
\end{aligned}$$