Chapter 6 Lecture Notes

Greg Knapp

March 30, 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:

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

2 Euler's Theorem

Refresher and Motivation

- Recall Fermat's Little Theorem: If p prime, then for any $a \not\equiv 0 \mod p$, $a^{p-1} \equiv 1 \mod p$.
- This is going to be our preferred statement of FLT this term.
- Fact (to be proven later in chapter 10): This theorem is unimprovable. For every prime p, there exists $a \not\equiv 0 \mod p$ so that $a^x \not\equiv 1 \mod p$ when $1 \leqslant x < p - 1$.
- Let's talk about how to generalize it to a composite modulus.
- A good modulus to try is 9. If I have $a \not\equiv 0 \mod 9$, for what x will I have $a^x \equiv 1 \mod 9$?
  - 1 to any power is $1 \mod 9$
  - Powers of b mod 9:

x	1	2	3	4	5	6	7	8
0^x	0	0	0	0	0	0	0	0
1^x	1	1	1	1	1	1	1	1
2^x	2	4	8	7	5	1	2	4
3^x	3	0	0	0	0	0	0	0
4^x	4	7	1	4	7	1	4	7
5^x	5	7	8	4	2	1	5	7
6^x	6	0	0	0	0	0	0	0
7^x	7	4	1	7	4	1	7	4
8^x	8	1	8	1	8	1	8	1

  - Question 1: for which values of b is it possible for $b^x \equiv 1 \mod 9$?
  - Answer 1: When $(b, 9) = 1$
  - Question 2: When $(b, 9) = 1$, what powers of x yield $b^x \equiv 1 \mod 9$?
  - Answer 2a: When $(b, 9) = 1$, $b^6 \equiv 1 \mod 9$.
  - Answer 2b: When $(b, 9) = 1$, the smallest x so that $b^x \equiv 1 \mod 9$ has $x \mid 6$. This follows from the cyclic nature of raising things to powers.
- **Prop:** Suppose that $m > 0$ and that $b^x \equiv 1 \mod m$ for some $x \geqslant 0$. Then $(b, m) = 1$.

- Proof:
  - Suppose there is a prime p with $p \mid m$ and $p \mid b$.
  - Then $p \mid b^x$
  - Also, $p \mid m \mid b^x - 1$
  - But then $p \mid b^x - (b^x - 1) = 1$, a contradiction
  - Hence $(b, p) = 1$
- So if we want to generalize Fermat's Little Theorem, we'd better focus solely on the b with $(b, m) = 1$. Those are the ones that we can raise to a power and get 1.
- For example, when $m = 9$, we only care about base values
- Next question: why is $b^6 \equiv 1 \mod 9$ for all b with $(b, 9) = 1$?
- Where is the 6 coming from???
- To be seen...

The Euler Phi Function

- For any m, recall that we previously defined $(\mathbb{Z}\,/\,m\mathbb{Z}) = \{0, 1, \ldots, m-1\}$ as our standard, complete set of residues
- But we also allowed ourselves the flexibility of other complete sets of residues for the purpose of proofs
- Now we want to define the subset of $(\mathbb{Z}\,/\,m\mathbb{Z})$ whose elements are relatively prime to m
- **Def:** Define $(\mathbb{Z}\,/\,m\mathbb{Z})^\times := \{b \in \mathbb{Z}\,/\,m\mathbb{Z} : (b, m) = 1\}$
- **Ex:** $(\mathbb{Z}\,/\,9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$
- **Ex:** $(\mathbb{Z}\,/\,5\mathbb{Z})^\times = \{1, 2, 3, 4\}$
- **Ex:** $(\mathbb{Z}\,/\,p\mathbb{Z})^\times = \{1, 2, \ldots, p-1\}$ when p is prime
- **Def:** Define $\varphi(m) := \#\,(\mathbb{Z}\,/\,m\mathbb{Z})^\times$
- Note the use of phi and varphi
- **Ex:** $\varphi(9) = 6$, $\varphi(5) = 4$, $\varphi(p) = p - 1$ when p is prime
- **Def:** Most generally, define a <u>reduced residue system modulo m</u> to be a set S so that:
  - $|S| = \varphi(m)$
  - The elements of S are pairwise incongruent modulo m
  - For each $b \in S$, $(b, m) = 1$
- **Ex:** $\{1, 2, 4, 5, 7, 8\}$ is a reduced residue system modulo 9. It is not a reduced residue system modulo 10 (because 2 is not relatively prime to 10) nor is it is a reduced residue system modulo 7 (because $1 \equiv 8 \mod 7$ for instance)
- **Ex:** Another reduced residue system mod 9 is $\{10, 2, 4, 5, 7, 8\}$.
- More generally, we can replace any number in $(\mathbb{Z}\,/\,m\mathbb{Z})^\times$ with something it's congruent to mod m:
- **Ex:** Suppose that $m > 1$, $(a, m) = 1$, and $b \equiv a \mod m$. Show that $(b, m) = 1$.
  - Suppose that $p \mid m$ and $p \mid b$ for some prime p.
  - Since $a \equiv b \mod m$, there exists $k \in \mathbb{Z}$ so that $a - b = km$, i.e. $a = km + b$.

- But then $p \mid b$ and $p \mid m$, so $p \mid a$.
- Contradiction, so no such p exists.
- Hence, $(b, m) = 1$

- **Prop:** If $\{r_1, \ldots, r_{\varphi(m)}\}$ is a reduced residue system modulo m and $(a, m) = 1$, then $\{ar_1, \ldots, ar_{\varphi(m)}\}$ is also a reduced residue system modulo m.
- Proof:
  - Claim 1: ar_i is relatively prime to m.
  - If $p \mid m$ is prime, then $p \nmid a$ (since a and m are relatively prime) and $p \nmid r_i$ (since r_i and m are relatively prime), so $p \nmid ar_i$.
  - So no prime factor of m is also a factor of ar_i. Hence $(ar_i, m) = 1$.
  - Claim 2: $ar_i \equiv ar_j \mod m$ implies $i = j$.
  - Divide both sides by a since $(a, m) = 1$.
  - Note that $r_i \equiv r_j \mod m$ implies $i = j$ since $\{r_1, \ldots, r_{\varphi(m)}\}$ is a reduced residue system
  - Claim 3: $\#\{ar_1, \ldots, ar_{\varphi(m)}\} = \varphi(m)$
  - Trivial
- **Thm:** If $m > 0$ and $a \in \mathbb{Z}$ has $(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \mod m$
- Proof:
  - Let $(\mathbb{Z}/m\mathbb{Z})^\times = \{r_1, \ldots, r_{\varphi(m)}\}$.
  - Since a is relatively prime to m, $S = \{ar_1, \ldots, ar_{\varphi(m)}\}$ is a reduced residue system as well
  - Hence, $(ar_1)(ar_2)(ar_3) \ldots (ar_{\varphi(m)}) \equiv r_1 r_2 \cdots r_{\varphi(m)} \mod m$
  - Divide each side by all the r_i (since they are relatively prime to m) and get $a^{\varphi(m)} \equiv 1 \mod m$

Examples

- **Ex:** Find an inverse for 3 modulo 14
  - Note that $(\mathbb{Z}/14\mathbb{Z})^\times = \{1, 3, 5, 9, 11, 13\}$, so $\varphi(14) = 6$
  - Then $3^6 \equiv 1 \mod 14$, so 3^5 is an inverse for 3 mod 14.
  - $3^2 \equiv 9 \mod 14$
  - $3^4 \equiv 81 \equiv 11 \mod 14$
  - $3^5 \equiv 33 \equiv 5 \mod 14$
  - Of course, we could have done this by inspection, but this would be better for larger numbers
- Note how this compares to the naive algorithm for inverting a mod m. There are two possible naive algorithms to check here:
  1. Test every number $1, \ldots, m$
  2. Construct $(\mathbb{Z}/m\mathbb{Z})^\times$ and test each of the $\varphi(m)$ members
- Compare to: compute $\varphi(m)$ and then raise a to the $\varphi(m) - 1$
- Since raising to the $\varphi(m) - 1$ takes less than $\varphi(m) - 1$ multiplications (using repetetive squaring), and $\varphi(m)$ is easy to compute where $(\mathbb{Z}/m\mathbb{Z})^\times$ is hard to compute, this is quite efficient.
- **Ex:** Show that if a and m are positive integers with $(a, m) = (a - 1, m) = 1$, then $1 + a + a^2 + \cdots + a^{\varphi(m)-1} \equiv 0 \mod m$
  - Note that $\left(1 + a + a^2 + \cdots + a^{\varphi(m)-1}\right)(a - 1) = a^{\varphi(m)} - 1 \equiv 0 \mod m$
  - Since $(a - 1)$ is relatively prime to m, it must be the case that $m \mid 1 + a + \cdots + a^{\varphi(m)-1}$