Hensel's Lemma, existence of generators, quadratic residues

Andres Buritica

Once again, p is a prime and n is a positive integer throughout.

1 Hensel's Lemma

Let

$$P(x) = a_0x^0 + \cdots + a_nx^n$$

be a polynomial. We define the *derivative*

$$P'(x) = a_1x^0 + 2a_2x^1 + 3a_3x^3 + \cdots + na_nx^{n-1}.$$

Let r be an integer such that $P(r) \equiv 0 \pmod{n}$ but $\gcd(P'(r), n) \neq 0$. Prove that for any positive integer m, there is a unique s mod n^m such that $s \equiv r \pmod{n}$ and $P(s) \equiv 0 \pmod{n^m}$.

The case where $n = p$ is prime is most common. In this case, the condition $P(r) \equiv 0 \pmod{p}$ and $P'(r) \not\equiv 0 \pmod{p}$ is equivalent to r being a single root of P mod p. That is, $(x - r) \mid P(x)$ but $(x - r)^2 \nmid P(x)$.

2 Existence of generators

Let p be an odd prime.

- There exists a generator mod p.
- There exists a generator mod p^2.
- There exists a generator mod p^k for any positive integer k.
- There exists a generator mod $2p^k$ for any positive integer k.
- There exists a generator mod 2^k iff $k \leq 2$.
- If $n = xy$, where x and y are coprime and larger than 2, then there does not exist a generator mod n.

3 Quadratic residues

Assume there exists a generator mod n. An element $x \in \mathbb{Z}_n^*$ can be written as y^k for $y \in \mathbb{Z}_n^*$ iff $\operatorname{ord}_n(x) \gcd(\varphi(n), k) \mid \varphi(n)$.

If x can be written as y^2 for $y \in \mathbb{Z}_n^*$, then we say that x is a *quadratic residue (QR)* mod n. Note that 0 is not a QR mod n.

Prove that x is a QR mod n iff both

- $x \equiv 1 \pmod{\gcd(8, n)}$, and
- for each odd prime $p \mid n$, x is a QR mod p.

Hence, we now restrict ourselves to considering QRs mod p. Define the *Jacobi symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & a \text{ is a QR mod } p \\ -1 & \text{otherwise} \end{cases}.$$

- (Euler's criterion) Prove that $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Hence, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
- (Gauss' Lemma) Let $a \in \mathbb{Z}_p^*$, and let $S \subseteq \mathbb{Z}_p^*$ such that $x \in S \iff -x \notin S$. Let $T = \{ay : y \in S\}$. Then $\left(\frac{a}{p}\right) = (-1)^{|T \setminus S|}$.
- Find $\left(\frac{2}{p}\right)$.

Finally, there is quadratic reciprocity which we won't prove today. Let p and q be distinct odd primes. Then,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

4 Problems

1. Let k and n be positive integers such that n is odd. Prove that there is an integer a such that $a^{32} \equiv (n+1)^3 \pmod{n^k}$.
2. Prove that for any prime p and positive integer a with $p \nmid a$ there are at least $p-1$ solutions in $\mathbb{Z}_p$ to $x^2 + y^2 \equiv a \pmod{p}$.
3. Let p be prime and let a and b be positive integers such that $p \nmid b$. Prove that there exists a positive integer n such that $p^a \mid n^n - b$.
4. If $p > 3$ is a prime such that $\varphi(p-1) > \frac{p-1}{3}$, prove that there are two consecutive generators mod p.
5. Let p be a prime and let n be a positive integer with $p \nmid n$. Find

$$\sum_{i=1}^{p} \left(\frac{i^2 + n}{p}\right).$$

6. Let $p > 3$ be a prime and let a, b, c be integers with $a \neq 0$. Suppose that $ax^2 + bx + c$ is a perfect square for p consecutive integers x. Prove that $p \mid b^2 - 4ac$.

7. Let P be a nonconstant polynomial with integer coefficients. Prove that for any integer m there exist an integer n and a prime p such that $p^m \mid P(n)$.

8. Let $a_1, a_2, a_3, \ldots$ be a sequence of integers, such that for any positive integers n and k, the quantity
$$\frac{a_n + a_{n+1} + \cdots + a_{n+k-1}}{k}$$
is always the square of an integer. Prove that all a_is are equal.

5 Homework

1. Find the least residue of the product of $(4-x) \bmod p$, where x runs over all residues mod p except the quadratic residues.

2. Find all positive integers k such that for all positive integers n, there exist a prime p and positive integers x and y for which $\gcd(x, y) = 1$ and $p^n \mid \frac{x^k - y^k}{x - y}$.

3. Find all completely multiplicative functions $f : \mathbb{N} \to \mathbb{R}$ such that for all $a, b \in \mathbb{N}$, at least two of $f(a), f(b), f(a+b)$ are equal.

   Note: This problem was set as homework in lecture 2. However, no one found all of the solutions — for example, $f(x) = \left(\frac{x}{5}\right)$ is a solution.