Number Theory I
Spring 2018

Assignment 13.2
Due April 25

Exercise 1. Let p be an odd prime and $b \in \mathbb{Z}$ coprime to p. Suppose that b is a quadratic nonresidue of p. Use the complete multiplicativity of the Legendre symbol to show that every integer $a \in \mathbb{Z}$ coprime to p is either a quadratic residue of p or congruent $\pmod{p}$ to the product of b and a quadratic residue of p. [*Suggestion:* If a is a quadratic nonresidue, consider the congruence $bx \equiv a \,(\mathrm{mod}\ p)$.]

Exercise 2. Let p be an odd prime. In class we gave a constructive proof that $\left(\frac{a}{p}\right) = 1$ implies a is a square $\pmod{p^m}$ for all $m \in \mathbb{N}$. We can give a nonconstructive proof using Euler's Criterion as follows.

- **a.** If $\left(\frac{a}{p}\right) = 1$, explain why we can write $a^{(p-1)/2} = 1 + kp$ for some $k \in \mathbb{Z}$.
- **b.** Use induction to prove that $(1+kp)^{p^{m-1}} \equiv 1 \,(\mathrm{mod}\ p^m)$ for $m \geq 1$.
- **c.** Put parts **a** and **b** together to conclude that a is a square $\pmod{p^m}$ for all $m \in \mathbb{N}$.

Exercise 3. Let p be a prime (not necessarily odd). Given $a \in \mathbb{Z}$ we define

$$\nu_p(a) = \max\{n \in \mathbb{N}_0 \,|\, p^n | a\},$$

the *p-adic valuation of a*. Since $p^n | 0$ for all $n \in \mathbb{N}_0$, we set $\nu_p(0) = \infty$.

- **a.** Show that for all $a, b \in \mathbb{Z}$, $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.
- **b.** Let $r \in \mathbb{Q}$ and write $r = \frac{a}{b}$ (not necessarily reduced). Define $\nu_p(r) = \nu_p(a) - \nu_p(b)$. Use part **a** to show that $\nu_p(r)$ is well-defined, i.e. if we also have $r = \frac{c}{d}$, then $\nu_p(c) - \nu_p(d) = \nu_p(a) - \nu_p(b)$. [*Suggestion:* How can you tell when two fractions are equal?]
- **c.** For $r \in \mathbb{Q}$ define the *p-adic absolute value* of r by

  $$|r|_p = p^{-\nu_p(r)}.$$

  Show that $|\cdot|_p$ has the usual properties of an absolute value, namely for all $r, s \in \mathbb{Q}$:

  - **i.** $|r|_p \geq 0$ and $|r|_p = 0$ if and only if $r = 0$;
  - **ii.** $|rs|_p = |r|_p |s|_p$;
  - **iii.** $|r+s|_p \leq |r|_p + |s|_p$.

  [*Suggestion:* For **iii** show that $|\cdot|_p$ actually satisfies the (stronger) *ultrametric inequality*, $|r+s|_p \leq \max\{|r|_p, |s|_p\}$.]