(*October 15, 2011*)

Number theory exercises/discussion 03

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/˜garrett/

(Were due Mon, 10 Oct 2011.)

[number theory 03.1] A $\sqrt{-1}$ exists in $\mathbb{Q}_5$.

Since $\mathbb{Z}/5^\times$ is cyclic of order 5, the (fourth cyclotomic) polynomial $f(x) = x^2 + 1$ has a zero mod 5, for example, 2, and $f'(2) = 4 \neq 0$ mod 5. Thus, Hensel's lemma produces a Cauchy sequence $2, \ldots$ converging to a zero of $f(x)$ in $\mathbb{Z}_5 \subset \mathbb{Q}_5$.

[number theory 03.2] A primitive 11^{th} root of unity exists in $\mathbb{Q}_{23}$.

The polynomial $f(x) = (x^{11} - 1)/(x - 1)$ has a zero x_1 mod 5, with $x_1 \neq 1$ mod 5. Without determining x_1 explicitly, apart from it's not being 1 or 0 mod 23, computing mod 23,

$$f'(x_1) \;=\; \frac{11x_1^{10}}{x_1 - 1} - \frac{x_1^{11} - 1}{(x_1 - 1)^2} \;=\; \frac{11x_1^{10}}{x_1 - 1} \;=\; \frac{11x_1^{11}}{x_1(x_1 - 1)} \;=\; \frac{11}{x_1(x_1 - 1)} \;\neq\; 0 \bmod 23$$

Thus, Hensel's lemma produces a Cauchy sequence $x_1, \ldots$ converging to a zero of $f(x)$ in $\mathbb{Z}_{23} \subset \mathbb{Q}_{23}$.

[number theory 03.3] Addition, multiplication, and inversion (away from 0) are *continuous* on $\mathbb{Q}_p$.

The arguments simplify somewhat if the discreteness of the norm is exploited, but the underlying reason for this continuity resides in some algebraic identities and the triangle inequality. Fix $x, y \in \mathbb{Q}_p$. Continuity of addition is immediate: for $|x - x'|_p$ and $|y - y'|_p$ small,

$$|(x + y) - (x' + y')|_p \;\le\; |x - x'|_p + |y - y'|_p$$

can be made as small as we want. Slightly more complicatedly,

$$xy - x'y' \;=\; (x - x')y + (y - y')x' \;=\; (x - x')y + (y - y')(x' - x) + (y - y')x$$

which can be made as small as we want. Finally, for $x, x' \neq 0$,

$$\frac{1}{x} - \frac{1}{x'} \;=\; \frac{x' - x}{xx'} \;=\; \frac{x' - x}{x(x' - x) + x^2} \;=\; \frac{x' - x}{x^2}\frac{1}{1 - \frac{x - x'}{x}} \;=\; \frac{x' - x}{x^2}\Big(1 + \frac{x - x'}{x} + \big(\frac{x - x'}{x}\big)^2 + \ldots\Big)$$

For $|x - x'|_p$ small enough so that $|(x - x')/x|_p < 1$, the geometric series converges. Thus, with x fixed, making the leading $x' - x$ smaller makes $1/x - 1/x'$ smaller. ///

[number theory 03.4] Determine p-adic convergence of the usual power series $e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots$.

First, observe that the power p^ℓ of p dividing $n!$ is bounded by

$$\ell \;\le\; \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \ldots$$

because there are at most n/p integers less than n and divisible by p, at most n/p^2 numbers less than n and divisible by p^2, etc. Thus,

$$\mathrm{ord}_p\, n! \;\le\; \frac{n \cdot \frac{1}{p}}{1 - \frac{1}{p}} \;=\; \frac{n}{p - 1}$$

Since Cauchy's criterion is necessary *and sufficient* p-adically, the sum converges when the terms go to 0. The n^{th} term has p-adic size

$$\Big|\frac{x^n}{n!}\Big|_p \;\le\; \frac{|x|_p^n}{p^{-n/(p-1)}} \;=\; (|x|_p \cdot p^{1/(p-1)})^n$$

This goes to 0 if and only if

$$|x|_p \;<\; p^{-1/(p-1)}$$

For *odd* rational p, requiring $|x|_p < 1$ already implies $|x|_p \le p^{-1} < p^{-1/(p-1)}$. For $p = 2$, we need the stronger $|x|_p < p^{-1}$. ///

[number theory 03.5] * (Starred problems are optional.) Show that there are only finitely-many quadratic extensions of $\mathbb{Q}_p$. In fact, for p odd, there are exactly *three*, while there are exactly 7 quadratic extensions of $\mathbb{Q}_2$.

This uses p-adic exponential and log. Observe that

$$\log(1-x) \;=\; x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + \ldots$$

converges p-adically for $|x|_p < 1$. For p odd and $|x|_p < 1$, also $|e^x - 1|_p < 1$. Then it makes sense to claim that exp and log invert each other:

$$x \;=\; \log(e^x) \qquad\qquad 1-x \;=\; e^{\log(1-x)} \qquad\qquad (p\text{-adically, odd } p, \text{ for } |x|_p < 1)$$

For $p = 2$, arguments to exp and log must be slightly more constrained.

The quadratic field extensions K of a field k not of characteristic 2 are in bijection with $k^\times/(k^\times)^2$, by $k(\sqrt{D}) \leftrightarrow D \bmod (k^\times)^2$.

For rational p, given $\alpha \in \mathbb{Q}_p^\times$, multiplication by a suitable power of p makes $|p^\ell \alpha|_p$ either 1 or $1/p$.

For *odd* rational p, we claim that units $\eta \in \mathbb{Z}_p^\times$ with $\eta = 1 \bmod p$ are *squares*. Indeed, using exp and log,

$$\sqrt{1+x} \;=\; e^{\frac{1}{2}\cdot\log(1+x)} \qquad\qquad (p\text{-adically, odd } p, \text{ for } |x|_p < 1)$$

For two units η, η', if $\eta = \eta' \bmod p$ then $\eta^{-1}\cdot\eta' \in 1 + p\mathbb{Z}_p$, so η and η' differ multiplicatively by a square. Thus, the question of $\mathbb{Z}_p^\times$ mod squares reduces to $(\mathbb{Z}_p/p\mathbb{Z}_p)^\times = \mathbb{Z}/p^\times$ mod squares, which has exactly two elements, since $\mathbb{Z}/p^\times$ is cyclic of even order.

Thus, for odd rational p, letting η_o be a non-square p-adic unit, irredundant representatives for $\mathbb{Q}_p^\times$ mod squares are $1, \eta_o, p$, and $\eta_o p$.

For $p = 2$, the greater fragility of exp and log, and role of $1/2$ in square-root taking, give the more-constrained

$$\sqrt{1+8x} \;=\; e^{\frac{1}{2}\cdot\log(1+8x)} \qquad\qquad (2\text{-adically, for } |x|_2 \le 1)$$

This reduces to $\mathbb{Z}/8^\times$ modulo squares, which has 4 representatives, since $\mathbb{Z}/8^\times$ is a $2,2$-group. Thus, $\mathbb{Q}_2^\times$ mod squares has 8 representatives. ///
