Math 620, Fall, 1999
Homework Set 5: Consequences of Minkowski's Theorem and Related Topics
Selected Solutions

3. This problem relates to the field $K = \mathbb{Q}(\sqrt{5})$.

(a) Show that K has class number 1, i.e., that the ring of integers R in K is a PID.

Solution. Since $5 \equiv 1 \pmod 4$, the discriminant of R is just 5. So the Minkowski bound shows that every ideal class in $C(R)$ is represented by an ideal $0 \neq I \lhd R$ with $\|I\| < \frac{2}{4}\sqrt{5} = 1.118 < 2$. But this forces $\|I\| = 1$, hence $I = R$ principal. So $C(R)$ is trivial and R is a PID.

(b) What prime numbers $p \in \mathbb{N}$ can be written in the form $x^2 - 5y^2$, x, $y \in \mathbb{Z}$? (Hint: $x^2 - 5y^2 = N_{K/\mathbb{Q}}(x + y\sqrt{5})$. First see for what primes $\pm p$ can be written in the indicated form; then try to resolve the question of signs.)

Solution. First let's dispose of one exceptional case: $5 = 5^2 - 5 \cdot 2^2$, so 5 is of the indicated form. This is the only prime ramified in R. Since $[K : \mathbb{Q}] = 2$, for any other prime p, there are only two possibilities: either p is inert in R, and then p cannot be the norm of any element of R, or else pR splits as a product of two (distinct, since we're in the unramified case) prime ideals. Since R is a PID, in the latter case, we have $(p) = (\alpha)(\sigma(\alpha))$ for some $\alpha \in R$, (since the two prime ideal factors of (p) must both be principal and must be conjugate to one another under the Galois automorphism $\sigma : \sqrt{5} \to -\sqrt{5}$). So when p splits, we must have $x^2 - 5y^2 = N_{K/\mathbb{Q}}(x + y\sqrt{5}) = \pm p$, where $\alpha = x + y\sqrt{5}$. Here x and y are either both integers or both odd integers divided by 2.

Now $R = \mathbb{Z}[\theta]$ with $\theta = \frac{1+\sqrt{5}}{2}$. Note that θ is a unit with norm $\frac{1-5}{2^2} = -1$. The minimal polynomial of θ is $x^2 - x - 1$, which is irreducible mod 2, and thus 2 is inert. For odd primes p, since 2 is invertible mod p, p splits exactly when 5 has a square root mod p, i.e., when $\left(\frac{5}{p}\right) = +1$. By quadratic reciprocity, this happens if and only if $\left(\frac{p}{5}\right) = +1$, or when $p \equiv \pm 1 \pmod 5$, whereas when $p \equiv \pm 2 \pmod 5$, p cannot split and so p cannot be of the form $x^2 - 5y^2$ with x, $y \in \mathbb{Z}$.

There is just one remaining issue. We have seen that when $p = 2$ or p is odd and $p \equiv \pm 2 \pmod 5$, then p cannot be of the form $x^2 - 5y^2$ with x, $y \in \mathbb{Z}$. When $p \equiv \pm 1 \pmod 5$, then we must have a solution of $x^2 - 5y^2 = \pm p$, but with x and y only *half-integers*, *a priori*. But since $2 + \sqrt{5}$ is a unit in R with norm -1, we can always multiply $x + y\sqrt{5}$ by $2 + \sqrt{5}$ if necessary to get a solution of $x^2 - 5y^2 = p$. And if x and y were already integers, this doesn't change that, so we are done. Otherwise, since p is odd, x and y must both be odd multiples of $\frac{1}{2}$, say $a/2$ and $b/2$ with a and b odd. Note that $\frac{3+\sqrt{5}}{2}$ is a unit of norm 1 and that

$$\left(\frac{a + b\sqrt{5}}{2}\right)\left(\frac{3 + \sqrt{5}}{2}\right) = \frac{(3a + 5b) + (a + 3b)\sqrt{5}}{4}.$$

If $a \equiv b \equiv 1 \pmod 4$ or if $a \equiv b \equiv 3 \pmod 4$, this now lies in $\mathbb{Z}[\sqrt{5}]$ and so we have an integer solution of $x^2 - 5y^2 = p$. On the other hand, if $a \equiv 1$ and $b \equiv 3 \pmod 4$, or *vice versa*, then we replace $3 + \sqrt{5}$ by $3 - \sqrt{5}$ in this argument, and we still get an integer solution of $x^2 - 5y^2 = p$. To summarize, $x^2 - 5y^2 = p$ has an integer solution if $p = 5$ or if $p \equiv \pm 1 \pmod 5$, but not if $p \equiv \pm 2 \pmod 5$.