Tentamenskrivning i Algebraisk talteori 03-01-18

Lösningar

F.1 Baker, p.10-11.

F.2 Generalisation of the idea in the proof that there are infinitely many primes $q \equiv 1 \pmod 4$. Namely, we assume that there are only finitely many primes $\equiv 1 \pmod p$, say $q_1, ..., q_n$. We then consider the number

$$N = \left(2 \cdot \prod_{i=1}^{n} q_i\right)^p + 1.$$

N is odd, hence not divisible by 2 or by any q_i. But if q is any prime dividing N, then $\zeta = \sqrt[p]{N-1}$ is an element of order $2p$ in $(\mathbf{Z}/q\mathbf{Z})^\times$, so $2p$ divides the order of this group, namely $q - 1$. In other words, $q \equiv 1 \pmod{2p}$, equivalently $q \equiv 1 \pmod p$, since q is odd.

F.3 (i) Proposition 24 from my 2000 lecture notes.
(ii) See p.44-45 of Koblitz' book 'An introduction to number theory and cryptography'. I gave this as a handout in class.

F.4 (i) I will omit the detailed computations. With the help of Theorem 37 and relations (107), (108) from my 2000 lecture notes, you may compute that there are precisely three reduced forms, namely $f_1 = x^2 + 9y^2$, $f_2 = 2x^2 + 2xy + 5y^2$ and $f_3 = 3x^2 + 3y^2$. Note that the third of these is an imprimitive form.

(ii) Denote the given form by f_0. Prop. 48(i) implies that the primes p represented by some form of discriminant -36 are those for which either $4p \mid -36$ or $\left(\frac{-36}{p}\right) = 1$. The former condition is satisfied only by $p = 3$. Since 36 is a perfect square, the latter condition is equivalent to $\left(\frac{-1}{p}\right) = 1$, and hence is satisfied if and only if $p \equiv 1 \pmod 4$. The imprimitve form f_3 represents only multiples of 3 and hence no prime other than 3 itself. It is also easy to see that f_1 (resp. f_2) represents no number congruent to 2 (resp. 1) modulo 3. We conclude that f_1 (resp. f_2) represents all primes congruent to 1 (resp. 5) modulo 12.

The form f_0 is primitive and, modulo 3, is congruent to $2x^2 + xy + 2y^2$, from which we also easily see that it cannot represent any integer congruent to 1 modulo 3. Hence, f_0 must be equivalent to f_2 and represent all primes congruent to 5 modulo 12.

F.5 Approximately Satser 103 and 104 in my 2000 lecture notes.

F.6 Instead of writing out the solution, let me refer you to Theorem 4.21 in the book of Stewart and Tall, which is where I got this exercise from !!