Tentamenskrivning i Algebraisk talteori 03-01-18

Lösningar

F.1 (ii) If $n = n_1 n_2$ then any solution (x, y, z) to Fermat's Theorem for the power n gives the solution $(x^{n_1}, y^{n_1}, z^{n_1})$ to the theorem for the power n_2. Since every $n > 3$ can be written as a product $n_1 n_2$, where n_2 is either 4 or an odd prime, the result follows.
(iii) Theorem 4.2 in my supplementary lecture notes for 2002.

F.2 Exact same idea as in the proof that there are infinitely many primes $p \equiv 3 \pmod 4$. Namely, we assume that there are only finitely many ODD primes $\equiv 2 \pmod 3$, say $p_1, ..., p_n$. We then consider the number

$$N = 3\left(\prod_{i=1}^{n} p_i\right) + 2.$$

Since $N \equiv 2 \pmod 3$, it must have at least one prime factor congruent to 2 (mod 3). But N is not divisible by any p_i, and neither is it divisible by 2, since N is odd. This is a contradiction.

F.3 p.33 in my 2000 lecture notes and Chapter 4 of Baker.

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 two reduced forms, namely $x^2 + 6y^2$ and $2x^2 + 3y^2$.

(ii) One may apply suitable matrix transformations and see that the form $x^2 + 14xy + 55y^2$ can be reduced to the form $x^2 + 6y^2$. Another, probably simpler, way to see this is by checking that neither form can represent integers $\equiv 2 \pmod 3$. Similarly, the form $2x^2 + 3y^2$ represents no integer $\equiv 1 \pmod 3$.

In any case, the point is that our form represents the same integers as the form $x^2 + 6y^2$, and represents no integer $\equiv 2 \pmod 3$.

Now the problem can be easily solved using Prop. 48(i), which implies that the primes p represented by some form of discriminant -24 are those for which either $4p \mid -24$ or $\left(\frac{-24}{p}\right) = 1$. The former condition is satisfied only by $p = 2, 3$. Using Prop. 23 and Gauβ reciprocity, we find that the latter condition is satisfied by primes $p \equiv 1, 5, 7, 11 (\text{mod } 24)$.

Applying the mod-3 condition above, and noticing that $p = 3$ is not represented by the form $x^2 + 6y^2$, we conclude that our form represents all $p \equiv 1$ or $7 \pmod{24}$.

F.5 (i) See the handout I gave from Chapters 6,7 of the book by Stewart and Tall.
(ii) See the same handout or, for an alternative proof, pages 39-40 of Baker.

F.6 The result is that the sum equals $|G|$ if $2g = 0$, and is zero otherwise. This follows immediately from Prop. 6.3(i) and the fact that $[\chi(g)]^2 = \chi(2g)$. Pretty simple really !

F.7 A (concise as usual) proof of the fact that the limit is $3/\pi^2$ can be read in Baker, p.13-14.