Tentamenskrivning i Algebraisk talteori 01-04-07

Lösningar

F.1 Firstly, if n is a prime, then $k_n = n - 1$, that is

$$(p-1)! \equiv -1 \pmod{p}.$$

PROOF : The numbers $\{1, ..., p-1\}$, with the exception of $p-1$, are grouped in pairs $x, x^{-1} \pmod{p}$.

Next, if $n = 4$ then $k_4 = 2$, that is $3! \equiv 2 \pmod{4}$.

Finally I claim that, if n is composite and > 4, then $k_n = 0$, i.e.: that for $n > 4$ and composite we have

$$(n-1)! \equiv 0 \pmod{n}.$$

PROOF : Let p be a prime divisor of n and suppose $p^l \parallel n$. We must show that p^l divides $(n-1)!$. If $l = 1$ then, since n is not prime, we have $p < n$ and indeed p divides $(n-1)!$. So suppose that $l > 1$. It clearly suffices to have $lp < n$, and hence suffices to have

$$lp < p^l. \tag{1}$$

It's easy to prove (by induction, for example), that (1) holds unless $p = l = 2$, which corresponds to the exceptional case $n = 4$. q.e.d.

F.2 **(i)** Dirichlet's approximation theorem, p.43 in Baker or p.128 in my notes.

F.3 **(i)** Sats 16, s.21 in my notes.

(ii) Suppose otherwise. We have

$$\frac{1}{\zeta(s)} = \sum \frac{\mu(n)}{n^s} = \sum \frac{\mu(n)/\sqrt[4]{n}}{n^{s-1/4}}.$$

If the partial sums of the numerator are bounded, then Dirichlet's criterion implies that the series converges uniformly in any half-plane $\mathrm{Re}(s) > 1/4+\delta$, and hence, by Weierstraß' theorem, defines an analytic function in $\mathrm{Re}(s) > 1/4$. That is, $1/\zeta(s)$ is analytic in $\mathrm{Re}(s) > 1/4$, hence has no poles there, which means that $\zeta(s)$ has no zeroes in the region. But this contradicts our knowledge that ζ has zeroes along the line $\mathrm{Re}(s) = 1/2$.

F.4 p.28-9 in Baker.

F.5 (i) We first of all seek a solution to the congruence

$$h^2 \equiv 185 \pmod{4 \cdot 17}$$

and find that

$$7^2 = 185 - 2 \cdot (4 \cdot 17)\,.$$

This implies (see Sats 47, p.63 and its' proof) that the form $17x^2+7xy-2y^2$ has discriminant 185 and represents 17 in $(x\ y) = (1\ 0)$. It remains to reduce the form. Its' matrix is

$$A = \begin{pmatrix} 17 & 7/2 \\ 7/2 & -2 \end{pmatrix}.$$

If we take

$$M_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix},$$

then one checks that

$$(M_1M_2)^T A(M_1M_2) = \begin{pmatrix} -2 & 1/2 \\ 1/2 & 23 \end{pmatrix},$$

which is the matrix of the reduced form $-2x^2 + xy + 23y^2$. This form represents 17 in

$$\begin{pmatrix} x \\ y \end{pmatrix} = (M_1M_2)^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -2 \\ -1 \end{pmatrix}.$$

(ii) For example, the form $f(x,y) = xy$ represents every positive integer, with $f(n,1) = n$.

REMARK : It is perhaps interestign to note that there is no such form of a non-square discriminant. For suppose the discriminant is d. By Prop. 48, p.68, it suffices to find an odd prime p such that $\left(\frac{d}{p}\right) = -1$. By quadratic reciprocity, this is equivalent to finding a prime satisfying a finite number of congruences. Such primes exist, by Dirichlet's theorem on arithmetic progressions (See **F.1** on the January exam).

F.6 Theorem 73, p.95 in my notes.

F.7 **(i)** Theorem 55, p.75 in my notes, and Baker p.39-40 for a complete proof.

(ii) For any natural number x, we have $x^2 \equiv 0, 1$ or $4 \pmod 8$. It follows easily that no number of the form $8n + 7$ can be written as the sum of three or fewer squares.

F.8 **(i)** A ring A is *Noetherian* if it has no infinite ascending chains of ideals or, equivalently, if every ideal is finitely-generated as an A-module.

A ring A is *local* if it has exactly one maximal ideal.

(ii) **(a)** $A = \mathbf{Z}/N\mathbf{Z}$ where $N = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37$.

(b) A polynomial ring over $\mathbf{C}$ in infintely many variables is non-Noetherian (See supplementary exercise no. 17(ii)). Localising at an appropriate maximal ideal gives a non-Noetherian local ring.

(c) The polynomial ring $\mathbf{C}[x]$ in one variable is Noetherian (from algebraic structures you know it is a PID). But it has the infinite descending chain of ideals

$$(x) \supset (x^2) \supset (x^3) \supset \cdots$$