MAN 640 : Taltaori

Tentamen 170105

Lösningar

F.1 The possible orders of an element x of $\mathbf{F}_{31}^{\times}$ are all the divisors of $30 = 2 \cdot 3 \cdot 5$, namely 1,2,3,5,6,10,15 and 30. x is a primitve root if and only if x has order 30. The number of primitive roots is $\phi(30) = (2-1)(3-1)(5-1) = 8$, corresponding to the 8 (all prime) numbers in $[1, 30]$ which are relatively prime to 30, namely : 1,7,11,13,17,19,23,29. Hence, if x is any primitive root, then the complete list of primitive roots is given by

$$x, x^7, x^{11}, x^{13}, x^{17}, x^{19}, x^{23}, x^{29} \ (\mathrm{mod}\ 30). \tag{1}$$

We find a primitve root by trial-and-error. Note immediately that 2 is not a primitive root, since $2^5 = 32 \equiv 1 \ (\mathrm{mod}\ 31)$. On the other hand, let's look at 3. We have

$$3^2 \equiv 9, \quad 3^3 = 27 \equiv -4, \ \Rightarrow \ 3^5 = 3^2 \cdot 3^3 \equiv 9 \cdot (-4) \equiv -5.$$

From these we further deduce that

$$\begin{aligned} 3^6 = 3^3 \cdot 3^3 &\equiv 16, \\ 3^{10} = 3^5 \cdot 3^5 &\equiv 25 \equiv -6, \\ 3^{15} = 3^{10} \cdot 3^5 &\equiv (-6) \cdot (-5) = 30 \equiv -1. \end{aligned}$$

Hence, 3 has order 30, and is a primitive root. The full list of primitive roots thus consists of the appropriate powers of 3, as in (1). We compute

$$\begin{aligned} 3^7 = 3^5 \cdot 3^2 &\equiv (-5) \cdot 9 = -45 \equiv -14 \equiv 17, \\ 3^{11} = 3^{10} \cdot 3 &\equiv (-6) \cdot 3 = -18 \equiv 13, \\ 3^{13} = 3^{11} \cdot 3^2 &\equiv 13 \cdot 9 = 117 \equiv 24, \\ 3^{17} = 3^{15} \cdot 3^2 &\equiv (-1) \cdot 9 \equiv 22, \\ 3^{19} \equiv 3^{17} \cdot 3^2 &\equiv (-9) \cdot 9 = -81 \equiv -19 \equiv 12, \\ 3^{23} = 3^{15} \cdot 3^5 \cdot 3^3 &\equiv (-1) \cdot (-5) \cdot (-4) = -20 \equiv 11, \\ 3^{29} \equiv 3^{-1} &\equiv -10 \equiv 21. \end{aligned}$$

Thus, the complete list of primitive roots modulo 31 is

$$3, 11, 12, 13, 17, 21, 22, 24 \pmod{31}.$$

F.2 Theorem 4 in my lecture notes.

F.3 Let $\mathcal{Q}$ and $\mathcal{N}$ denote the sets of quadratic residues and non-residues respectively, modulo p. Since $p \equiv 3 \pmod 4$ we have that

$$x \in \mathcal{Q} \Leftrightarrow p - x \in \mathcal{N}. \tag{2}$$

Let $\mathcal{S} := \{1, 2, ..., \frac{p-1}{2}\}$. By definition of m we have (all congruences are modulo p)

$$\left[\frac{1}{2}(p-1)\right]! = \left(\prod_{x \in \mathcal{S} \cap \mathcal{Q}} x\right) \cdot \left(\prod_{x \in \mathcal{S} \cap \mathcal{N}} x\right) \equiv (-1)^m \cdot \left(\prod_{x \in \mathcal{S} \cap \mathcal{Q}} x\right) \cdot \left(\prod_{x \in \mathcal{S} \cap \mathcal{N}} p - x\right).$$

But by (2),

$$\left(\prod_{x \in \mathcal{S} \cap \mathcal{Q}} x\right) \cdot \left(\prod_{x \in \mathcal{S} \cap \mathcal{N}} p - x\right) = \prod_{x \in \mathcal{Q}} x,$$

i.e.: each quadratic residue in $[1, p)$ appears exactly once. Finally, when $p \equiv 3 \pmod 4$, the product of all quadratic residues is $\equiv 1 \pmod p$, since the quadratic residues occur in pairs $x, x^{-1} \pmod p$, and $p - 1$, which is its' own inverse, does not appear in the product.

F.4 Theorem 25 in my lecture notes.

F.5 It suffices to prove the result for primitive triples. Let (x, y, z) be any such triple and WLOG, assume y is odd. Then, by Theorem 5, there exist positive integers $a < b$ such that $\mathrm{GCD}(a, b) = 1$ and

$$x = 2ab, \qquad y = b^2 - a^2, \qquad z = b^2 + a^2. \tag{3}$$

Note that $60 = 2^2 \cdot 3 \cdot 5$, so to prove that a number is divisible by 60, it suffices to prove that it is divisible by each of 4,3 and 5.

First, since $\mathrm{GCD}(x, y, z) = 1$, it is clear from (3) that a and b must have opposite parity (otherwise each of x, y and z would be even). In other words, exactly one of a and b is even, and this implies that x is divisible by 4. Thus xyz is also divisible by 4.

Second, if either a or b is divisible by 3, then so is x, hence so also is xyz. Otherwise $a^2 \equiv b^2 \equiv 1 \pmod{3}$, hence y is divisible by 3 in this case. Thus xyz is divisible by 3 in all cases.

Finally, if either a or b is divisible by 5, then so is x, hence also xyz. Otherwise, $a^2 \equiv \pm b^2 \equiv \pm 1 \pmod{5}$, so that exactly one of $b^2 \pm a^2$ is divisible by 5. Thus xyz is also divisible by 5 in all cases, and the proof is complete.

F.6 (i) Page 72 in my lecture notes.
(ii) Sats 31 in my lecture notes.

F.7 (i) Let $\{a, b, c\}$ be a reduced form of discriminant -27. Since $b^2 - 4ac = -27$ is odd, we must have b odd. Since the form is reduced we have

$$0 < a \leq \sqrt{\frac{-d}{3}} \Rightarrow a \in \{1, 2, 3\}.$$

If $a = 1$ then, since $b \in (-a, a]$, the only possibility is $b = 1$. This gives $c = 7$, so we have the form $\{1, 1, 7\}$.

If $a = 2$ then $b \in \{\pm 1\}$, in which case $c = (b^2 + 27)/4a = 28/8 \notin \mathbf{Z}$, so we get nothing there.

Finally, if $a = 3$, then $b \in \{\pm 1, 3\}$. If $b = \pm 1$ then $c = 28/12 \notin \mathbf{Z}$. But if $b = 3$, then $c = 3$, so we get the form $\{3, 3, 3\}$.

We conclude that there are two reduced forms of discriminant -27, namely

$$x^2 + xy + 7y^2 \quad \text{and} \quad 3x^2 + 3xy + 3y^2.$$

(ii) Denote the given form as $f(x, y) = \{103, 73, 13\}$. We apply the following sequence of transformations to reduce the form :

$$\begin{aligned} S &: \{103, 73, 13\} \mapsto \{13, -73, 103\}, \\ T^3 &: \{13, -73, 103\} \mapsto \{13, 5, 1\}, \\ S &: \{13, 5, 1\} \mapsto \{1, -5, 13\}, \\ T^3 &: \{1, -5, 13\} \mapsto \{1, 1, 7\}. \end{aligned}$$

Hence f is equivalent to the reduced form $x^2 + xy + 7y^2$. To work out the variable substitution which accomplishes this transformation, we compute

$$ST^3ST^3 = (ST^3)^2 = \left[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}\right]^2 = \begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix}^2 = \begin{pmatrix} -1 & -3 \\ 3 & 8 \end{pmatrix}.$$

Hence the desired variable substitution is

$$f(-x - 3y, 3x + 8y) = x^2 + xy + 7y^2.$$

F.8 (i) For $\mathrm{Re}(s) > 1$, the following representation is valid :

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}.$$

(ii) Theorem 27 in my lecture notes.