Matematiska Institutionen, KTH

Tentamen SF2728, Talteori, June 1 2026, 08.00-13.00.

Examinator: Pär Kurlberg (08-7906582). Jourhavande lärare: Kirsti Biggs (08-7907832).

NOTE: No calculators or other aids may be used. For full points correct and well presented arguments are necessary.

1. (4p) Use the Jacobi symbol to determine (514/1093).

As $514 = 2 \cdot 257$ quadratic reciprocity gives

$$(514/1093) = (2/1093) \cdot (257/1093) = (-1)^{\frac{1093^2-1}{8}} \cdot (-1)^{\frac{256}{2} \cdot \frac{1092}{2}} \cdot (1093/257).$$

Since $1093 \equiv 5 \mod 8$ we have $(-1)^{\frac{1093^2-1}{8}} = -1$ and we easily see that $(-1)^{\frac{256}{2} \cdot \frac{1092}{2}} = 1$, and thus $(514/1093) = -(1093/257)$.

Since $1093 \equiv 65 \mod 257$ we find that

$$(1093/257) = (65/257) = (-1)^{32 \cdot 128}(62/65)$$

$$= (-3/65) = (-1/65) \cdot (3/65) = (3/65) = (-1)^{\frac{2}{2}\frac{64}{2}}(2/3) = -1$$

Thus $(514/1093) = 1$.

2. (4p) Find the minimal polynomial, over $\mathbb{Q}$, for $\sqrt{2} + \sqrt{3}$.

Let $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ and define

$$f(x) := (x - (\sqrt{2} + \sqrt{3}) \cdot (x - (\sqrt{2} - \sqrt{3}) \cdot (x - (-\sqrt{2} + \sqrt{3}) \cdot (x - (-\sqrt{2} - \sqrt{3})$$

$$= ((x - \sqrt{2})^2 - 3) \cdot ((x + \sqrt{2})^2 - 3) = (x^2 - 2)^2 - 6(x^2 + 2) + 9$$

$$= x^4 - 4x^2 + 4 - 6x^2 - 12 + 9 = x^4 - 10x^2 + 1$$

If f is irreducible then f is indeed the minimal polynomial for $\sqrt{2} + \sqrt{3}$; to do this it suffices to show that $[K : \mathbb{Q}] = 4$.

As $(3 - 2)/(\sqrt{3} + \sqrt{2}) = \sqrt{3} - \sqrt{2}$ we find that both $\sqrt{3} - \sqrt{2}, \sqrt{3} - \sqrt{2} \in K$, and thus $\sqrt{2}, \sqrt{3} \in K$. As $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ (since $\sqrt{2}$ is irrational) and $\mathbb{Q}(\sqrt{2}) \subset K$ we have $[K : \mathbb{Q}] = 2, 4$, to rule out the former it is enough to show that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. If $3 = (a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}$ for $a, b \in \mathbb{Q}$ we must have $ab = 0$ since $\sqrt{2}$ is irrational. If $b = 0$ then $a^2 = 3$, contradicting that $\sqrt{3}$ is irrational. If $a = 0$, then we find $2b^2 = 3$ which implies that $(2b)^2 = 6$, contradicting that that $\sqrt{6}$ is irrational.

Hence $x^4 - 10x^2 + 1$ is the sought minimal polynomial.

3. (4p) Let $p \equiv 1 \mod 4$ be a prime. Show that there exists $x, y \in \mathbb{Z}$ such that $x^2 + y^2 = p$.

Since $p \equiv 1 \mod 4$ and $\mathbb{F}_p^\times$ is cyclic there exists $x \in \mathbb{Z}$ such that $x^2 + 1 \equiv 0 \mod p$; in particular we have the $\mathbb{Z}[i]$-factorization $(x + i)(x - i) = p$. We recall that $\mathbb{Z}[i]$ is a PID, hence a UFD. In particular, if p is irreducible we must have $p|x + i$ or $p|x - i$, but neither alternative is possible as any element of the form $p \cdot (a + ib)$ must have imaginary part divisible by p. Thus p is reducible and we can write $p = \pi\gamma$ where π is irreducible and γ is not a unit. Next we note that π, γ not units implies that $|N(\pi)| = |\pi|^2 \neq 1$ and $|N(\gamma)| = |\gamma|^2 \neq 1$. Thus, as $p^2 = N(p) = N(\pi)N(\gamma)$ we find that $N(\pi) = |\pi|^2 = p$; writing $\pi = a + ib$ with $a, b \in \mathbb{Z}$ we have shown that $p = a^2 + b^2$.

4. (4p) Let χ be a nontrivial multiplicative character on $\mathbb{F}_p$ (with the standard convention that $\chi(0) = 0$), and let $g(\chi) = \sum_{t=0}^{p-1} \chi(t)\zeta^t$ where $\zeta = e^{2\pi i/p}$. Show that $|g(\chi)| = \sqrt{p}$.

Using the change of variables $s = ut$, together with $\overline{\chi(t)} = \chi(t^{-1})$, we find that

$$|g(\chi)|^2 = \sum_{s,t \not\equiv 0 \mod p} \chi(s)\overline{\chi(t)}\zeta^{s-t} = \sum_{u,t \not\equiv 0 \mod p} \chi(u)\zeta^{t(u-1)}$$

Now, for $u \equiv 1 \mod p$, we have $\sum_{t \not\equiv 0 \mod p} \zeta^{t(u-1)} = p - 1$, whereas for $u \not\equiv 1 \mod p$, we have $\sum_{t \not\equiv 0 \mod p} \zeta^{t(u-1)} = -1$ (since $1 + \zeta + \ldots + \zeta^{p-1} = 0$), and thus

$$|g(\chi)|^2 = p - 1 - \sum_{u \not\equiv 0,1} \chi(u) = p - 1 - (-1) = p$$

since $\sum_{u \not\equiv 0} \chi(u) = 0$ and $\chi(1) = 1$. Hence $|g(\chi)| = \sqrt{p}$.

5. (4p) Let $d > 0$ be a square free integer. Show that the equation $x^2 - dy^2 = 1$ has a nontrivial solution (i.e., such that $y \neq 0$.)

See book.

6. (4p) Let $p \equiv 1 \mod 3$ be an odd prime. Show, using Jacobi sums, that the equation $x^3 + y^3 \equiv 1 \mod p$ has at least $p/10$ solutions for all sufficiently large p.

With χ denoting a non-trivial cubic character, the number of solutions to $x^3 = a$ is given by by $\sum_{i=0,2} \chi^i(a)$ (with the convention that $\chi^0(0) = 1$.) Thus the number of solutions equals

$$\sum_{i,j=0}^{2} \sum_{a+b=1} \chi^i(a)\chi^j(b) = \sum_{i,j=0}^{2} J(\chi^i, \chi^j)$$

For $i = j = 0$ we have $J(\chi^i, \chi^j) = p - 2$; for all other choices we have $|J(\chi^i, \chi^j)| \leq \sqrt{p}$. Hence, the number of solutions equals $p + O(\sqrt{p})$, which for p sufficiently large is, $\geq p/10$.