MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

WS 2004/2005
Feb. 3, 2005

Algebraic Number Theory
Solution of Problem 45

Problem 45

a) Decompose the polynomial $\overline{\Phi}_7(X) = \sum_{k=0}^{6} X^k \in \mathbb{F}_{29}[X]$ into a product of linear factors.

b) Write 29 as a product of six prime elements of the ring $\mathbb{Z}[e^{2\pi i/7}]$.

Solution. a) Since $\mathbb{F}_{29}^*$ has 28 elements, there exists a subgroup $G \subset \mathbb{F}_{29}^*$ of order 7. The elements $x \in G \smallsetminus \{1\}$ are then the zeros of $\overline{\Phi}_7(X)$. Now 2 is a primitive root modulo 29 (since $2^4 \not\equiv 1$ and $2^7 \not\equiv 1 \bmod 29$). Therefore $16 = 2^4$ generates the subgroup G,

$$G = \{16^k : k = 0, 1, \ldots, 5\} = \{1, 16, 24, 7, 25, 23, 20\}.$$

Therefore

$$\begin{aligned}\Phi_7(X) &\equiv (X-16)(X-24)(X-7)(X-25)(X-23)(X-20)\\ &\equiv (X+13)(X+5)(X-7)(X+4)(X+6)(X+9) \bmod 29\end{aligned}$$

b) By a theorem proved in the course, one has

$$(29) = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3 \cdot \mathfrak{p}_4 \cdot \mathfrak{p}_5 \cdot \mathfrak{p}_6,$$

with

$$\mathfrak{p}_k = (29, \zeta - x_k) \subset \mathbb{Z}[\zeta], \quad \zeta = e^{2\pi i/7},$$

where x_k are the roots of $\Phi_7(X) \bmod 29$. To decompose 29 into a product of 6 primes in $\mathbb{Z}[\zeta]$ amounts to finding generators ξ_k of $\mathfrak{p}_k$. We deal only with the ideal

$$\mathfrak{p} := (29, \zeta + 4),$$

since the other ideals are obtained from this one by applying the automorphisms of the Galois group. A generator of $\mathfrak{p}$ must have norm 29, since $\mathbb{Z}[\zeta]/\mathfrak{p} \cong \mathbb{F}_{29}$. By computer aided search one finds that

$$\xi := 1 + \zeta + 2\zeta^2 = 29 + (-7 + 2\zeta)(\zeta + 4)$$

has indeed $\mathrm{N}(\xi) = 29$. The other primes are obtained from ξ by applying the automorphisms $\sigma_\nu : \zeta \mapsto \zeta^\nu$, $\nu = 1, 2, \ldots, 6$. Therefore

$$29 = \xi_1 \cdot \ldots \cdot \xi_6$$

with the primes

$$
\begin{aligned}
\xi_1 &= \sigma_1(\xi) = \xi = 1 + \zeta + 2\zeta^2, \\
\xi_2 &= \sigma_2(\xi) = 1 + \zeta^2 + 2\zeta^4, \\
\xi_3 &= \sigma_3(\xi) = -1 - 2\zeta - 2\zeta^2 - \zeta^3 - 2\zeta^4 - 2\zeta^5, \\
\xi_4 &= \sigma_4(\xi) = 1 + 2\zeta + \zeta^4, \\
\xi_5 &= \sigma_5(\xi) = 1 + 2\zeta^3 + \zeta^5, \\
\xi_6 &= \sigma_6(\xi) = -\zeta - \zeta^2 - \zeta^3 - \zeta^4 + \zeta^5.
\end{aligned}
$$

Of course the decomposition is unique only up to order and multiplication by units (there are many units in $\mathbb{Z}[\zeta]$!).
