Prof. Friedrich Eisenbrand
Nicolai Hähnle

Discussions from: April 19, 2011

Computer Algebra

Spring 2011

Assignment Sheet 5

Exercises marked with a ⋆ can be handed in for bonus points. Due date is May 10.

Let R be a commutative ring. Then $\omega \in R$ is a *primitive n-th root of unity* if

1. $\omega^n = 1$,
2. $n \in R^\star$, and
3. for all divisors t of n, $t \neq n$, the element $(\omega^t - 1) \in R$ is not a zero divisor.

Exercise 1 (⋆)
Let $R = \mathbb{Z}_{21}$. For every element $x \in R$, determine whether it is in $R^\star$ (that is, whether it is invertible) and whether it is a zero divisor.[1] Determine the order of every element $x \in R^\star$.[2] Finally, determine which elements are primitive roots of unity.

Exercise 2
Let $R = \mathbb{Z}_7$ and $S = \mathbb{Z}_{11}$ and consider the product ring $T = R \times S \cong \mathbb{Z}_{77}$. Consider the following example about how roots of unity in the product ring *don't* relate to roots of unity in the component rings (compare also the next exercise!).

1. Show that $\omega_1 = 2$ is a primitive 3-rd root of unity modulo 7.
2. Show that $\omega_2 = 4$ is a primitive 5-th root of unity modulo 11.
3. Let $\omega = 37$. Prove that $\omega \equiv \omega_1 \pmod 7$ and $\omega \equiv \omega_2 \pmod{11}$ and that ω is a 15-th root of unity modulo 77 (that is, $\omega^{15} \equiv 1 \pmod{77}$, and $\omega^k \not\equiv 1 \pmod{77}$ for $1 \leq k < 15$).
4. Prove that ω is *not* a primitive root of unity modulo 77.

Exercise 3
Let R and S be commutative rings and consider their product ring $T = R \times S$. Let $\omega = (\omega_R, \omega_S) \in T$. Prove that ω is a primitive n-th root of unity if and only if ω_R and ω_S are primitive n-th roots of unity in R and S, respectively.

[1] But be careful not to over-generalize what you see. Consider also rings like $\mathbb{Z}$ or $k[x]$.
[2] The order is the smallest positive integer n such that $x^n = 1$.

Exercise 4 ($\star$)
Let R be a commutative ring and $\omega \in R$ such that $\omega^n = 1$ and $n \in R^\star$. Prove that the following are equivalent:

1. for all $k \in \mathbb{Z}$ such that n does not divide k, $(\omega^k - 1) \in R$ is not a zero divisor.
2. for all divisors t of n, $t \neq n$, the element $(\omega^t - 1) \in R$ is not a zero divisor.

Exercise 5
Let R be a ring with a primitive n-th root of unity $\omega \in R$. Prove:

1. ω^{-1} is a primitve n-th root of unity.
2. If n is even, then ω^2 is a primitive $(n/2)$-th root of unity. If n is odd, then ω^2 is a primitive n-th root of unity.
3. Let $k \in \mathbb{Z}$ and $d = n/\gcd(n,k)$. Then ω^k is a d-th root of unity.

Exercise 6
What is the number of primitive n-th roots of unity in $\mathbb{C}$?

Exercise 7
Let $n \in \mathbb{N}$. Show that 2 is a primitive $2n$-th root of unity modulo $2^n + 1$ if and only if n is a power of 2.

Exercise 8
Let $f = x^2 + 2x - 5$ and $g = x^2 + 3x + 2$. Let $N = 17$ and $\omega = 2 \in \mathbb{Z}_N$.

1. Show that ω is an 8-th primitive root of unity in $\mathbb{Z}_N$.
2. Use the discrete Fourier transform to compute $f(\omega^i)$ and $g(\omega^i) \mod N$, $i = 0 \ldots 7$.
3. Use the inverse discrete Fourier transform on $f(\omega^i)g(\omega^i)$. Can you use the result to find fg?