Berkeley Math Circle
IF GAUSS DID IT, YOU CAN TOO!

Sep. 2, 2014
Instructor: Paul Zeitz
(zeitzp@usfca.edu)

---

1 *Primitive Roots*. Let p be a prime. A non-trivial theorem states that there exists a *primitive root (modulo p)*, i.e., there exists an integer g such that $g^0, g^1, g^2, \ldots, g^{p-1}$ are the $p-1$ distinct positive residues (modulo p). The number g is sometimes also called a generator. You will have an opportunity to prove the primitive root theorem below. Meanwhile...

(a) Verify that 2 is a primitive root modulo 5.

(b) Verify that 2 is not a primitive root modulo 7, but 3 is.

(c) Verify that 3 is a primitive root modulo 17.

2 *Gauss's "Periods," specific case*. Let p be a prime (fixed in context). Let g be a primitive root (modulo p), also fixed. Let let e, f be positive integers such that $ef = p-1$. Define the function

$$P_f(z) := z + z^{g^e} + z^{g^{2e}} + \cdots + z^{g^{(f-1)e}}.$$

These functions are *only* useful if z is a pth root of unity. Let $\zeta = \cos(2\pi/p) + i\sin(2\pi/p)$. If you are familiar with Euler's theorem, you can also write $\zeta = e^{2\pi i/p}$. We will *always* assume that $z = \zeta^k$ for some integer k.

Consider the specific case $p = 17, g = 3$. Define

- $H_k := P_8(\zeta^{g^k})$ for $k = 0, 1$;
- $Q_k := P_4(\zeta^{g^k})$ for $k = 0, 1, 2, 3$;
- $E_k := P_2(\zeta^{g^k})$ for $k = 0, 1, 2, 3, 4, 5, 6, 7$,

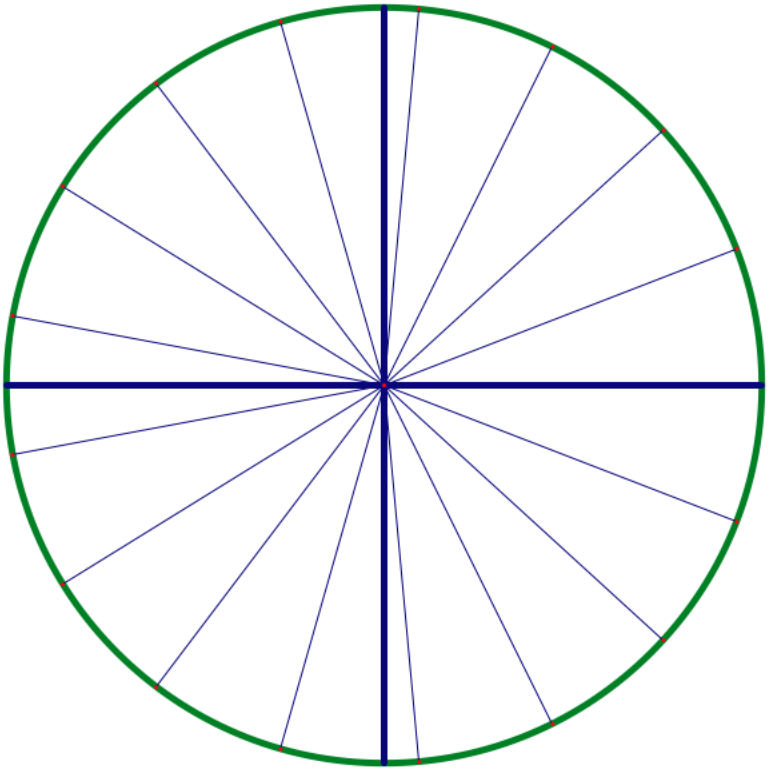
where the letters H, Q, E denote "half, quarter, eighth," respectively.

(a) For $k = 0, 1, \ldots, 15$, compute $P_{16}(\zeta^k)$.

(b) Write out a half-dozen of these H, Q, E expansions, both retaining the g-to-a-power notation and also with actual exponents (e.g. writing ζ^{g^6} and also ζ^{15}).

(c) Show that all of these numbers are real! Why?

(d) Carefully compute $H_0 + H_1$ and H_0^2 and H_1^2, and use these latter ones to compute $H_0 H_1$.



3 *Gauss's "Periods," general case*. Fix a prime p with primitive root g, and positive integers e, f whose product is $p-1$. Prove the following (remember that z must be pth root of unity):

(a) $P_f(z)^2 = \sum_{r=0}^{f-1} P_f(z^{1+g^{re}})$.

(b) If e is even, then $P_f(z) + P_f(z^{g^{e/2}}) = P_{2f}(z)$.

What is so great about these identities? How do they relate to the previous problem?

4 Use the ideas above to verify that

$$\cos\frac{2\pi}{17} = -\frac{1}{8} + \frac{1}{8}\sqrt{17} + \frac{1}{8}\sqrt{34-2\sqrt{17}} + \frac{1}{4}\sqrt{17+3\sqrt{17}-\sqrt{34-\sqrt{17}}-2\sqrt{34+2\sqrt{17}}},$$

and thus one can construct regular 17-gons with compass and straightedge!

5 *The Primitive Root Theorem*. There are many ways to prove this, all them involving at least some sophisticated ideas. The following problems sketch one direction. We will prove that there is a non-zero element g in Z_p (the integers modulo p) with *order* $p-1$. In other words, $g^{p-1} \equiv 1 \pmod{p}$, but $g^k \not\equiv 1 \pmod{p}$ for all positive k less than $p-1$. Clearly any g that satisfies this condition is a primitive root modulo p.

Our strategy will be to look at polynomials, both ordinary polynomials with integer coefficients and polynomials whose coefficients are elements of Z_p. We are always assuming that p is prime.

(a) *Foundational Ideas*.

1. Recall *Fermat's Little Theorem*: If a is nonzero, then $a^{p-1} \equiv 1 \pmod{p}$. Prove it!
2. Prove that if m is a prime, that an nth degree polynomial with integer coefficients has at most n roots in Z_m, but that this is not necessarily true (construct examples!) if m is not a prime.
3. Prove that if $a^n \equiv 1 \pmod{p}$, then the order of a must divide n. Consequently, the order of a must divide $n-1$.
4. Recall the *Fundamental Theorem of Arithmetic*, which states that integers have unique prime factorizations (up to order). The same theorem holds for polynomials. It can be proven in more or less the same way. Do it!

(b) *Primitive roots of unity and cyclotomic polynomials.*

1. An nth root of unity $\zeta = e^{2\pi ia/n}$ is called a *primitive* nth root of unity if n is the least positive integer such that $\zeta^n = 1$. Show that among the nth roots of unity, $\zeta = e^{2\pi ia/n}$ is a primitive nth root iff $a \perp n$, i.e. if a and n are relatively prime.
2. Define the **nth cyclotomic polynomial** $\Phi_n(x)$ to be the polynomial with leading coefficient 1 and degree $\phi(n)$ whose roots are the $\phi(n)$ different *primitive* roots of unity. Compute $\Phi_4(x), \Phi_{12}(x), \Phi_p(x)$ (for p prime).
3. Prove that $x^n - 1 = \prod_{d|n} \Phi_d(x)$.
4. Prove that the coefficients of $\Phi_n(x)$ are integers for all n. Must the coefficients only be ± 1?

(c) *Finally, the proof!*. The key idea is to look at cyclotomic polynomials in Z_p.

1. Look at $x^{p-1} - 1$ (modulo p). Explain why it has the (unique) factorization into linear factors:

$$x^{p-1} - 1 = \prod_{d|p-1} \Phi_d(x) = (x-1)(x-2)\cdots(x-(p-1))$$

.

2. We claim that all the roots of $\Phi_{p-1}(x)$ (modulo p) will be primitive roots. Note that this polynomial has exactly $\phi(p-1)$ roots in Z_p, where ϕ is the Euler function. Assume, to the contrary, that a is a root of $\Phi_{p-1}(x)$ and the order of a is d, where $d < p-1$. *Carefully* show that this produces a contradiction: the factorization of $x^{p-1}-1$ will contain $(x-a)$ in *two* places, which is impossible!