Algebra Autumn 2017
Frank Sottile
13 September 2017 Third Homework

Write your answers neatly, in complete sentences. Recopy your work before handing it in. Correct and crisp proofs are greatly appreciated; oftentimes your work can be shortened and made clearer.

Hand in for the grader Tuesday 19 September:

9. Let $x_1, \ldots, x_n$ be variables. Prove the following *Vandermonde identity* $\det(x_i^{j-1})_{i,j=1}^n = \prod_{1\le a<b\le n}(x_b - x_a)$. For example,

$$\det\begin{pmatrix} 1 & 1 & 1 & 1 \\ x_1 & x_2 & x_3 & x_4 \\ x_1^2 & x_2^2 & x_3^2 & x_4^2 \\ x_1^3 & x_2^3 & x_3^3 & x_4^3 \end{pmatrix} = (x_2-x_1)(x_3-x_1)(x_4-x_1)(x_3-x_2)(x_4-x_2)(x_4-x_3)\,.$$

10. Let G be a group of order $2n$. Show that G has at least one element of order 2.

    Suppose that n is odd. Show that if G is abelian then it has a unique element of order 2.

    Show that if G is the dihedral group of rigid symmetries of the regular n-gon, then is has n elements of order 2. (What if n is even?)

11. Let $m \ge 2$ be an integer. Set $\mathbb{Z}_m^* := \{k \in \mathbb{Z}_m \mid \gcd(k,m)=1\}$. These are the cosets of integers that are relatively prime to m.

    (a) Show that $\mathbb{Z}_m^*$ is the set of generators of the cyclic group $\mathbb{Z}_m$.

    (b) Show that $\mathbb{Z}_m^*$ is a group under multiplication modulo m. Define $\phi(m) := |\mathbb{Z}_m^*|$, the order of this group. This is Euler's *totient function*, also called Euler's ϕ-function.

    (c) Deduce Euler's Theorem. If $\gcd(a,m)=1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.
    (That is, m divides $a^{\phi(m)}-1$, equivalently, $a^{\phi(m)}=1$ as elements of $\mathbb{Z}_m$.)

    (d) Let p be a prime number and show that $\phi(p)=p-1$.

    Determine $\phi(p^n)$, where p is a prime and $n>0$ is an integer.

    Show that ϕ is multiplicative; if $a,b\in\mathbb{N}$ are relatively prime, ($\gcd(a,b)=1$), then $\phi(ab)=\phi(a)\cdot\phi(b)$.

    Deduce a formula for $\phi(m)$ in terms of the factorization of m into a product of powers of distinct primes. Express this in terms of m and its distinct prime divisors.

    (e) Deduce Fermat's Little Theorem from the last part. If p is any prime number and $a\in\mathbb{Z}$, then $a^p \equiv a \pmod{p}$.