Homework #5. Due on Thursday, October 3rd, 11:59pm on Canvas

Reading:

1. For this assignment: Online lecture 8 and 9. From Hungerford: 2.3, 4.1 and 4.2.
2. For next week's classes: Online lecture 10. From Hungerford: 4.2 and parts of 4.3, 5.1 and 7.1.

Online lectures are currently posted on the Spring 2016 webpage

`https://m-ershov.github.io/3354_Spring2016/`

Problems:

Preface to problem 1: Recall from the previous homework that for $n, k \in \mathbb{Z}$ with $0 \leq k \leq n$, the binomial coefficient $\binom{n}{k}$ is defined by $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ (where $0! = 1$). Also recall the binomial theorem: for every $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \ldots + \binom{n}{n-1} a b^{n-1} + \binom{n}{n} b^n.$$

Note that $\binom{n}{k}$ is always an integer – this is not obvious from definition, but it is (almost) obvious from the binomial theorem.

Problem 1: Suppose that p is prime and $0 < k < p$. Prove that $p \mid \binom{p}{k}$.
Hint: First prove the following lemma: Suppose that $n, m \in \mathbb{Z}$, p is prime, $m \mid n$, $p \mid n$ and $p \nmid m$. Then $p \mid \frac{n}{m}$ (this follows from Euclid's lemma).

Problem 2: In both parts of this problem p is a prime number.

(a) Prove the little Fermat's theorem: $n^p \equiv n \mod p$ for any $n \in \mathbb{N}$.
(b) Reformulate (a) as an equality in $\mathbb{Z}_p$. Your reformulation should be of the form "for all $x \in \mathbb{Z}_p$ we have $f(x) = 0$ where $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is a certain explicit function"

Hint for (a): Fix p and use induction on n. For the induction step use the result of Problem 1.

Problem 3: Let $X = \mathbb{R}^2$ (the set of ordered pairs of real numbers) and define a relation $\sim$ on X by

$$(x_1, y_1) \sim (x_2, y_2) \iff x_1 + y_1 = x_2 + y_2.$$

(a) Prove that $\sim$ is an equivalence relation.

(b) Describe equivalence classes with respect to $\sim$. **Hint:** there is a very easy geometric description if you think of elements of X as points on the Euclidean plane.

Problem 4: Define a relation $\sim$ on $\mathbb{Z}$ by

$$x \sim y \iff x^3 \equiv y^3 \mod 4.$$

(a) Prove that $\sim$ is an equivalence relation.
(b) Find the number of equivalence classes with respect to $\sim$ and describe (explicitly) each class.

Hint for (b): The equivalence classes with respect to $\sim$ are closely related to congruence classes mod 4. Once you figure out the relationship (and why it holds), it is fairly easy to finish the problem.

Problem 5: Let R be a commutative ring with 1 and $R[x]$ the ring of polynomials with coefficients in R. Prove the following properties of the degree function:

(a) $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$ for all $f, g \in R[x]$
(b) $\deg(f+g) = \max\{\deg(f), \deg(g)\}$ for all $f, g \in R[x]$ such that $\deg(f) \neq \deg(g)$
(c) $\deg(fg) \leq \deg(f) + \deg(g)$
(d) If R has no zero divisors (such R is called a domain), then $\deg(fg) = \deg(f) + \deg(g)$
(e) Find a specific n and $f \in \mathbb{Z}_n[x]$ such that f is non-constant (that is, $\deg(f) > 0$), but f is invertible. **Hint:** Part (d) (and what we proved earlier) yields certain restrictions on the possible values of n.

Problem 6: Let $f(x) = x^4 - 1$ and $g(x) = x^2 + 3x + 1$, and consider f and g either as polynomials in $\mathbb{Z}_5[x]$ or $\mathbb{Z}_7[x]$ (in both cases the coefficients of f and g should be interpreted as congruence classes mod 5 and mod 7, respectively). In both cases do the following:

(a) divide f by g with remainder
(b) Compute $gcd(f, g)$
(c) Find explicit polynomials $u(x)$ and $v(x)$ such that $gcd(f(x), g(x)) = f(x)u(x) + g(x)v(x)$.

Note: We will talk about gcd in class on Monday, Sep 30 (see also 4.2 in Hungerford), but the following information should be sufficient to solve this problem. If F is a field and $f(x), g(x) \in F[x]$, not both 0, $gcd(f(x), g(x))$ is defined to be the MONIC polynomial of largest possible degree which divides both $f(x)$ and $g(x)$ (a polynomial is called monic if its leading coefficient is 1). We will prove that $gcd(f(x), g(x))$ always exists and is unique.

Similarly to $\mathbb{Z}$, one can prove that $gcd(f(x), g(x))$ is the unique monic polynomial of smallest possible degree representable as $f(x)u(x) + g(x)v(x)$ for some $u(x), v(x) \in F[x]$. Moreover, one can find the gcd itself as well as u and v from the above representation using the Euclidean algorithm essentially in the same way as for $\mathbb{Z}$. The only real difference is that while in the case of $\mathbb{Z}$, gcd is the last nonzero remainder in the first part of the Euclidean algorithm, in the polynomial case the last nonzero remainder is a constant multiple of the gcd (to get the actual gcd, one just needs to divide that remainder by its leading coefficient).