Math 113 **Fall 2015**

Homework #10

Nikhil Unni

1. For each of the following use the modulo technique to show that the equation has no integer solutions.

   (a) $21x^2 - 36y = 44$

   We can show this has no integer solutions in $\mathbb{Z}_3$. The equation becomes:

   $$21x^2 - 36y \equiv 44(mod 3)$$
   $$0 - 0 \equiv 2$$
   $$0 \equiv 2$$

   ...which cannot be, regardless of our choice of x or y.

   (b) $3x^2 - 4y = 5$

   If we take solve this in mod 4 (admittedly not a prime modulo group) then we get:

   $$3x^2 - 4y \equiv 5(mod 4)$$
   $$3x^2 \equiv 1$$

   And looking at all the squares in mod 4:

   $$0^2 = 0$$
   $$1^2 = 1$$
   $$2^2 = 0$$
   $$3^2 = 1$$

   So $3x^2$ in mod 4 can only be 0 or 3, which is not 1. So there are no integer solutions in mod 4.

(c) $x^5 - 3y^5 = 2008$

If we solve this in mod 11 we'll get:

$$x^5 - 3y^5 \equiv 2008(mod 11)$$

$$x^5 - 3y^5 \equiv 6(mod 11)$$

Looking at all the powers of 5 in mod 11:

$$0^5 = 0$$

$$1^5 = 1$$

$$2^5 = 10$$

$$3^5 = 1$$

$$4^5 = 1$$

$$5^5 = 1$$

$$6^5 = 10$$

$$7^5 = 10$$

$$8^5 = 10$$

$$9^5 = 1$$

$$10^5 = 10$$

And looking at all the multiples of 3 of the possible power 5 values:

$$3 * 0 = 0$$

$$3 * 1 = 3$$

$$3 * 10 = 8$$

Looking at all the solutions of $\{0, 1, 10\} - \{0, 3, 8\}$, there's no way to get 6 in mod 11.
Therefore, there can be no integer solutions in mod 11.

2. Let $R = \mathbb{Q}[x]$.

(a) Prove that the set I of all polynomials in R which have 2 as a zero forms an ideal of R. Which of our adjectives for ideals (maximal, prime, principal) apply to I? Justify your answer.

First we show that I is an additive subgroup. We know that $f(x) = 0$ is in I, because all $q \in \mathbb{Q}$ are zeros of the 0 function. Then, for any $a, b \in I$:

$$a - b = (x-2)f_a(x) - (x-2)f_b(x) = (x-2)((f_a - f_b)(x))$$

We know that since 2 is a root of a and b, we can factor out $x-2$. So the subtraction ends up being a multiple of $x-2$ as well, meaning that 2 is a root of $a-b$, making it a valid element of I.

Next, we show it's an ideal. For $i \in I, r \in R$, $ir = ri$, since multiplication is commutative. Then:

$$ir = ((x-2)f_i(x)) * f_r(x)$$

$$ir = (x-2)(f_i(x)f_r(x))$$

This product, again, has $(x-2)$ as a factor, and thus has 2 as a root, making all $ir \in I$ as well.

From the next problem, we see that R/I is isomorphic to $\mathbb{Q}$, which is a field. Since I is maximal iff R/I is a field, and since $\mathbb{Q}$ is a field, we know that I is maximal. From the definition from the book, an element, a, is a zero of $f(x)$ iff $(x-a)$ is a factor of $f(x)$. Definition chasing, this means that all elements $(x-2)f(x) \in R$ make up I.

So, if we ever have an element $f(x)g(x) \in I$, if we split up $f(x)$ and $g(x)$ into its unique irreducible factors, $f(x)g(x)$ will be equivalent to $(x-2)f_1(x)g_1(x)f_2(x)g_2(x)\ldots$. So $(x-2)$ must have been a factor in either $f(x)$ or $g(x)$ (constant factors aside), meaning that if $fg(x) \in I$, either $f(x) \in I$ or $g(x) \in I$, making I prime (since $I \neq R$).

By the same definition of an element of I, all elements in I are of the form $(x-2)f(x)$. So we can say that I is generated by $\langle (x-2) \rangle$, making I a principal ideal.

(b) What familiar ring is R/I isomorphic to? Justify your answer.

Let $\phi : R \to \mathbb{Q}$, where $\phi(f(x)) \mapsto f(2)$, be the evaluation homomorphism at 2.
For some $f(x), g(x) \in R$:

$$\phi(f(x)g(x)) = f(2)g(2) = \phi(f(x))\phi(g(x))$$

$$\phi(f(x) + g(x)) = f(2) + g(2) = \phi(f(x)) + \phi(g(x))$$

$$\phi(1) = 1$$

So we have a valid ring homomorphism.

Then, we know that the kernel of ϕ is the set of all polynomials in R that map to 0 when evaluated at 2. And, by definition, these are the polynomials with 2 as a zero, or I. Also, we know that ϕ is onto, since we can just have $(x - a)$ as a term for all $a \in \mathbb{Q}$, so by the First Isomorphism Theorem of Rings, we know that $\mathbb{Q}$ is isomorphic to R/I.

3. Let $R = \mathbb{Q}[x, y]$, the ring of polynomials in two variables.

Just as a note – whenever I use $f(x)$ or $g(x)$ as examples of members of R, just know that $x \in \mathbb{Q} \times \mathbb{Q}$, and that it represents the x,y evaluation tuple, not just x... I just use it as shorthand for a generic polynomial in two variables.

(a) Prove that $I = \{f(x, y) \in R : f(1, 3) = f(2, -5) = 0\}$ is an ideal of R.

First we have to show it's an additive subgroup. We know that 0 is in I, since it will evaluate to zero regardless of the arguments. Then, for some $a, b \in I$:

$$(a - b)(1, 3) = a(1, 3) - b(1, 3) = 0 - 0 = 0$$

$$(a - b)(2, -5) = a(2, -5) - b(2, -5) = 0 - 0 = 0$$

So it is a valid additive subgroup.

Now we show it's a valid ideal in R. For $i \in I, r \in R$, $ir = ri$, since multiplication is commutative. Then:

$$(ir)(1, 3) = i(1, 3) * r(1, 3) = 0 * r(1, 3) = 0$$

$$(ir)(2, -5) = i(2, -5) * r(2, -5) = 0 * r(2, -5) = 0$$

So I is a valid ideal of R.

(b) Is I equal to the principal ideal $\langle(3x-y)(5x+2y)\rangle$ in R? Justify your answer.

It is not equal to that principal ideal, because we can find an element in I that is not the result of $(3x - y)(5x + 2y) * f(x) = (15x^2 + xy - 2y^2)f(x)$, for some $f(x) \in R$. If we choose our element to be $i = (3x^2 - y)(5x + 2y) = 15x^3 + 6x^2y - 5xy - 2y^2 \in I$, there's no way to find a multiple of the generator to get our element. It's a bit involved with a multivariate division algorithm, but if we

just look at the monomials, we know we'll need an x term with no coefficient to get $15x^3$ and a constant 1 to get $-2y^2$, but these create a conflict when trying to find terms that might generate $6x^2y$ and $-5xy$.

(c) Can you determine whether I is maximal and/or prime?

I is not maximal, since we can find a larger superset ideal. Let $J = \{f(x,y) \in R : f(1,3) = 0\}$. This is a valid ideal for the same reason that we just showed in part (a) (subtracting out all of the $(2,-5)$ evaluations). It is clearly a superset of I, since it contains all the evaluations where $(1,3) \mapsto 0$, and $(2,-5) \mapsto 0$, but it also has elements where $(2,-5) \mapsto c$, for some $c \in \mathbb{Q}$. So I cannot be maximal.

Also, it is not prime. If we have some $f(x), g(x) \in R$ where $(fg)(x) \in I$, then $(fg)(1,3) = 0$ and $(fg)(2,-5) = 0$. This means:

$$f(1,3) * g(1,3) = 0$$

$$f(2,-5) * g(2,-5) = 0$$

But if we had $f(x,y) = 3x - y$, and $g(x,y) = 5x + 2y$, then $(fg)(x) \in I$, but $f(x) \notin I$ and $g(x) \notin I$.