MATH 371 – Midterm I – October 3, 2013

1. (a) Use the Euclidean algorithm to find the greatest common divisor of 312 and 252, and two integers λ and μ satisfying $312\lambda + 252\mu = \gcd(312, 252)$.

(b) Find a polynomial $p(x) \in \mathbb{R}[x]$ such that $\langle p\rangle = \langle x^4 - 3x^3 - x + 3\,,\; x^3 - 2x^2 - 5x + 6\rangle \subset \mathbb{R}[x]$, and prove that the two ideals are equal.

(a)

i	-1	0	1	2	3
r_i	312	252	60	12	0
q_i	–	–	1	4	5
λ_i	1	0	1	-4	–
μ_i	0	1	-1	5	–

Therefore $\gcd(312, 252) = 12$ and $-4 \cdot 312 + 5 \cdot 252 = 12$.

(b)

i	-1	0	1	2
r_i	$x^4 - 3x^3 - x + 3$	$x^3 - 2x^2 - 5x + 6$	$3x^2 - 12x + 9$	0
q_i	–	–	$x - 1$	$\frac{1}{3}x + \frac{2}{3}$
λ_i	1	0	1	–
μ_i	0	1	$-x + 1$	–

Therefore $\gcd(x^4 - 3x^3 - x + 3\,,\; x^3 - 2x^2 - 5x + 6) = 3x^2 - 12x + 9$ and $3x^2 - 12x + 9 = 1 \cdot (x^4 - 3x^3 - x + 3) + (-x + 1) \cdot (x^3 - 2x^2 - 5x + 6)$.

Let $I = \langle x^4 - 3x^3 - x + 3\,,\; x^3 - 2x^2 - 5x + 6\rangle$. Then $I = \langle p\rangle$, where $p = 3x^2 - 12x + 9$. We have $x^4 - 3x^3 - x + 3 = \frac{1}{3}(x^2 + x + 1)(3x^2 - 12x + 9)$ and $x^3 - 2x^2 - 5x + 6 = \frac{1}{3}(x + 2)(3x^2 - 12x + 9$. Thus both generators of I are divisible by p, therefore $I \subset \langle p\rangle$. And from our gcd expression we have that $p \in I$, therefore $\langle p\rangle \subset I$. Putting these two inclusions together gives $I = \langle p\rangle$.

---

2. Let I and J be ideals in the the commutative ring R, with the property that $I + J = R$.

(a) Prove that $IJ = I \cap J$ (recall that IJ is the ideal *generated by* products of the form xy, with $x \in I$ and $y \in J$.

(b) Generalize the Chinese Remainder Theorem to this context: Prove that there is an isomorphism

$$\varphi\colon R/(I \cap J) \to R/I \times R/J.$$

(c) Give an example of a ring R and ideals I and J of R satisfying $IJ \neq I \cap J$.

(a) Suppose $x \in IJ$, then $x = \sum_{i=1}^{n} p_i q_i$ where $p_i \in I$ and $q_i \in J$ for all i. But we have $p_i q_i \in I$ (because I is an ideal and $p_i \in I$), and likewise we have $p_i q_i \in J$. Therefore $IJ \subset I \cap J$.

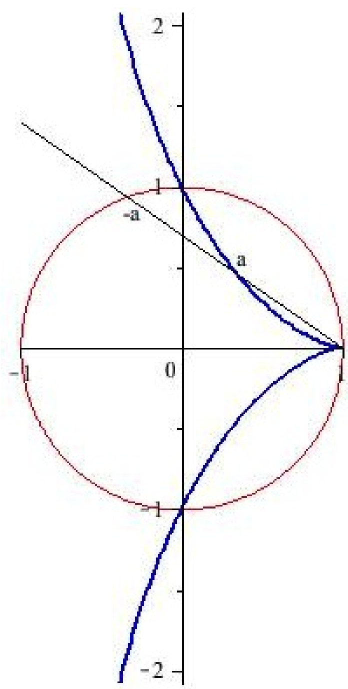
Now suppose $x \in I \cap J$. Since $I + J = R$, we have $1 \in I + J$, therefore there is $a \in I$ and $b \in J$ such that $a + b = 1$. Therefore $x = (a + b)x \in IJ$ since $ax \in IJ$ and $xb \in IJ$ (since x is in both I and J, $a \in I$ and $b \in J$). Therefore $I \cap J \subset IJ$. Putting the two inclusions together gives $I \cap J = IJ$.

(b) We'll find a surjective homomorphism $\overline{\varphi}$ from R to $R/I \times R/J$ with kernel $I \cap J$, and then the first isomorphism theorem (that the image of $\overline{\varphi}$ is isomorphic to $R/\ker\varphi$) will imply that φ is an isomorphism. The map $\overline{\varphi}$ will send $x \in R$ to the pair $([x]_I\,,\,[x]_J)$, where $[x]_I$ is the coset of I containing x and $[x]_J$ is the coset of J containing x. This is clearly a ring homomorphism (by the standard properties of cosets of ideals), and the kernel of R consists of all elements x with $[x]_I = I$ and $[x]_J = J$, so $x \in I \cap J$. This is just what we needed to complete the proof.

(c) Let $R = \mathbb{Z}$, and let $I = \langle 24 \rangle$ and $J = \langle 20 \rangle$. Any element in IJ must be a multiple of 480, so $IJ = \langle 480 \rangle$. But $I \cap J = \langle 120 \rangle$.

---

3. The *cissoid of Diocles* is an affine plane curve in $\mathbb{R}^2$. Diocles (around 180 B.C.) described the cissoid in a way that amounts to the following: Begin with the unit circle centered at the origin. For each a between -1 and 1, consider the line L that connects the point $(1,0)$ to the point $(-a, \pm\sqrt{1-a^2})$ on the unit circle (note the $-a$). The point on L with x-coordinate a is a point on the cissoid, and the cissoid is the locus of all such points:



(a) Prove that the cissoid is an affine variety by finding its equation in x and y.

(b) Prove that the cissoid is a *rational* affine variety by finding a rational parametrization of it.

(a) The line through $(-a, \sqrt{1-a^2})$ and $(1,0)$ has slope $-\sqrt{1-a^2}/(1+a)$ and is $y = -\dfrac{\sqrt{1-a^2}}{(1+a)}(x-1)$. The point at $x = a$ on this line has

$$y = -\frac{\sqrt{1-a^2}}{1+a}(a-1) = \frac{\sqrt{1-a^2}}{1+a}(1-a).$$

Therefore the point on the cissoid satisfies

$$y^2 = \frac{(1-x^2)(1-x^2)}{(1+a)^2} = \frac{(1-a)^3}{1+a}.$$

So the equation of the cissoid as an affine variety is $(1+x)y^2 = (1-x)^3$.

(b) Since the "interesting" point on the cissoid is $(1,0)$, we'll parametrize the cissoid by the slopes of lines through $(1,0)$. So assume $y = m(x-1)$. Then $(1+x)m^2(x-1)^2 = (1-x)^3$, i.e., $(1+x)m^2 = 1-x$. Solving for x gives first $(m^2+1)x = 1-m^2$, so

$$x = \frac{1-m^2}{m^2+1}.$$

And since $y = m(x-1)$, we get

$$y = m\left(\frac{(1-m^2)+(m^2+1)}{m^2+1}\right) = \frac{-2m^3}{m^2+1}.$$

---

4. Let R be a commutative ring, and suppose P is a prime ideal of R. Prove that if P contains no zero-divisors then R is an integral domain.

Suppose $xy = 0$ in R with $x \neq 0$. Since $0 \in P$ we must have either $x \in P$ or $y \in P$. But P contains no zero divisors, so if $x \in P$ then we must have $y = 0$, and if $x \notin P$ then we must have $y \in P$ and again $y = 0$. Since x and y were arbitrary, R must be an integral domain.

---

5. Suppose $n > 2$ is a composite number. We are going to find a criterion for n to be a Carmichael number as follows:

(a) Show that the condition $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$ implies the *Carmichael condition* $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}$ satisfying $\gcd(a,n) = 1$.

We already know from class that a Carmichael number n must have a prime factorization of the form $n = p_1p_2\cdots p_k$ where $k \geqslant 3$, p_i is odd for all i, and $p_i \neq p_j$ for $i \neq j$ (i.e., n is square-free). Now, suppose we have that n is odd, composite, square-free and $p-1 \mid n-1$ for all primes p that divide n, and let $a \in \mathbb{Z}$.

(b) Explain why, if $\gcd(a,p_i) = 1$, then $a^n \equiv a \pmod{p_i}$ (you'll need Fermat's little theorem and good old corollary 2).

(c) Now explain why, if $\gcd(a,p_1) \neq 1$ (so that we'd necessarily have $p_i \mid a$), then $a^n \equiv a \equiv 0 \pmod{p_i}$.

(d) Explain why (b) and (c) together imply $a^n \equiv a \pmod{n}$.

Putting this all together, we have that a number n that is a product of at least three distinct primes $n = p_1\cdots p_k$ such that $p_i - 1 \mid n-1$ for all i must be a Carmichael number. It is true (but requires a fact we don't yet have a proof for, namely that the multiplicative group $(\mathbb{Z}/\langle p\rangle)^*$ is a cyclic group) that all Carmichael numbers satisfy this condition. This gives a more efficient way to search for Carmichael numbers than trying all the numbers less than n satisfying $\gcd(a, n) = 1$ to make sure they satisfy $\boldsymbol{a}^{n-1} \equiv 1 \pmod{n}$. As an extra-credit assignment over the weekend, write a computer program that takes as input a list of all the prime numbers between 1000 and 3000, say, and uses this criterion to search for Carmichael numbers greater than a million.

(a) Since $\gcd(a, n) = 1$, there are λ and μ such that $\lambda a + \mu n = 1$. But then $1 - \lambda a = \mu n$, so $\lambda a \equiv 1 \pmod{n}$. Multiply both sides of $a^n \equiv a \pmod{n}$ by λ and get $\lambda a a^{n-1} \equiv \lambda a \pmod{n}$, and so $a^{n-1} \equiv 1 \pmod{n}$.

(b) If $\gcd(a, p_i) = 1$ then $a^{p_i - 1} \equiv 1 \pmod{p_i}$ by Fermat's little theorem. Since $p_i - 1 \mid n - 1$, we have $n - 1 = k_i(p_i - 1)$. Therefore

$$a^{n-1} = a^{k_i(p_i-1)} = (a^{p_i-1})^k \equiv 1^k \equiv 1 \pmod{p_i}.$$

(c) If $\gcd(a, p_i) \neq 1$, then $p_i \mid a$ since p_i is prime, and so $a \equiv 0 \pmod{p_i}$. And so $a^n \equiv 0 \equiv a \pmod{p_i}$.

(d) Since $p_i \mid a^n - a$ for all i, we have $(p_1 \cdots p_k) \pmod{a)^n} - a$ by repeated application of Corollary 2. In other words, $n \mid a^n - a$.