Prof. Bjorn Poonen
February 25, 2005

# MATH 160 MIDTERM SOLUTIONS

**(1)** *(5 pts. each) For each of (a)-(d) below: If the proposition is true, write TRUE. If the proposition is false, write FALSE. (Please do not use the abbreviations T and F, since in handwriting they are sometimes indistiguishable.) No explanations are required in this problem.*

*(a) There exist integers $x$ and $y$ satisfying $709x + 100y = 4$.*

TRUE, since $\gcd(709, 100) = 1$, which divides 4. (The gcd can be computed using the Euclidean algorithm, or by observing that the only prime factors of 100 are 2 and 5, neither of which divides 709.)

*(b) Starting from any two distinct points in the plane, it is possible to construct a regular 7-gon using straightedge and compass.*

FALSE, since 7 is not a Fermat prime. (Alternatively, if a regular 7-gon were constructible, it would follow that $e^{2\pi i/7}$ would be an algebraic number of 2-power degree, whereas in fact it has degree 6, being a zero of the irreducible polynomial $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.)

*(c) Starting from two points in the plane 1 unit apart, it is possible to construct a circle of radius $\sqrt{\sqrt{2} + \sqrt{3}}$ using straightedge and compass.*

TRUE, since $\sqrt{\sqrt{2} + \sqrt{3}}$ is a constructible number.

*(d) The equation $x^2 - 9y^2 = 1$ has infinitely many integer solutions.*

FALSE. (It's not Pell's equation, since 9 is a square.) The solutions have $x+3y = x - 3y = \pm 1$. This gives two linear systems, each of which gives one solution.

**(2)** *(30 pts.) Prove that there are infinitely many primes congruent to 2 modulo 3.*

Suppose there were only finitely many primes congruent to 2 modulo 3. Let $p_1, \ldots, p_s$ be all of them. Let $n = 3p_1 \cdots p_s - 1$. Since $n \equiv -1 \equiv 2 \pmod 3$, 3 does not divide $n$, and not all prime factors of $n$ are 1 mod 3. So we can pick a prime factor $q$ of $n$ that is 2 mod 3. Since $p_1, \ldots, p_s$ are all primes congruent to 2 mod 3, we have $q = p_i$ for some $i$. Then $q$ divides $3p_1 \cdots p_s = n + 1$ as well as $n$, so $q$ divides 1, which is impossible. This contradiction proves that there are infinitely many primes congruent to 2 modulo 3.

**(3)** *(30 pts.) Either find a parametrization of the rational solutions to $x^2 + 2y^2 = 7$, or prove that no rational solutions exist.*

We will prove that no rational solutions exist. Suppose that $(x, y)$ is a rational solution. Let $c \in \mathbb{Z}_{>0}$ be the least common denominator for $x$ and $y$. Thus $x = a/c$ and $y = b/c$ for some $a, b \in \mathbb{Z}$. Moreover, $\gcd(a, b, c) = 1$, since otherwise dividing $a, b, c$ by the gcd shows that $c$ is not the *least* common denominator.

Substituting $x = a/c$ and $y = b/c$ into $x^2 + 2y^2 = 7$ and multiplying by $c^2$ gives $a^2 + 2b^2 = 7c^2$. Thus $a^2 + 2b^2 \equiv 0 \pmod 7$.

If $b \equiv 0 \pmod 7$, then $a^2 \equiv -2b^2 \equiv 0 \pmod 7$, so 7 divides $a^2$, so 7 divides $a$, so $7^2$ divides $a^2$ and $b^2$, so $7^2$ divides $a^2 + 2b^2 = 7c^2$, so 7 divides $c^2$, so 7 divides $c$, so 7 is a common factor of $a, b, c$, contradicting $\gcd(a, b, c) = 1$.

If $b \not\equiv 0 \pmod 7$, then (denoting by $\bar{z}$ the image of $z \in \mathbb{Z}$ in the field $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$) we get $(\bar{a}/\bar{b})^2 + 2 = 0$ in $\mathbb{F}_7$, so $-2$ is a square in $\mathbb{F}_7$. But the squares in $\mathbb{F}_7$ are $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 2$ (and then $4^2 = (-3)^2 = 2$ and so on). So this case gives a contradiction too.

**(4)** *(20 pts.) Show that for any nonzero real number $a$, the projective closure of the plane curve $y^2 = ax^3$ is projectively equivalent to the projective closure of the curve $y = x^3$.*

The projective closures are given in homogeneous coordinates by $Y^2Z = aX^3$ and $YZ^2 = X^3$. The invertible linear substitution $(X, Y, Z) \mapsto (\sqrt[3]{a}X, Z, Y)$ transforms the second equation into the first.

This is the end! At this point, you may want to look over this sheet to make sure you have not omitted any problems. Check that your answers make sense! Please take this sheet with you as you leave.