Prof. Bjorn Poonen
October 5, 2001

# MATH 55 PRACTICE MIDTERM

*Do not write your answers on this sheet.* Instead please write your name, your student ID, your TA's name, your section time, and all your answers in your blue books. In general, you must show your work to get credit. Total: 100 pts., 75 minutes.

**(1)** For each of (a)-(g) 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) The circle $\{(x,y) : x \in \mathbb{R},\ y \in \mathbb{R}, \text{ and } x^2+y^2=1\}$ is a countable set.

(b) The propositions $p \to \neg q$ and $q \to \neg p$ are logically equivalent.

(c) If $p$ is a prime number, then there is a prime $q$ satisfying $p < q < p+6$.

(d) There exists a positive integer $m$ such that $30, 77, m$ are pairwise relatively prime.

(e) In the RSA cryptosystem, when Bob wants to send Alice a message, it is essential that Bob keeps his encryption method secret.

(f) $3^{405} \equiv 13 \pmod 7$.

(g) It is valid to deduce $\neg q$, if $\neg p$ and $p \to q$ have been proved already.

**(2)** Find a compound proposition involving $p, q, r$ that is true if and only if at least two of $p, q, r$ are false.

**(3)** Let $S$ be the subset of $\mathbb{N}$ defined recursively by

- $7 \in S$
- $10k \in S$ whenever $k \in S$, and
- $k-2 \in S$ whenever $k \in S$ and $k \geq 2$.

Describe $S$, and determine whether 107 is in $S$.

**(4)** For which real numbers $r$ is it true that

$$(4\lceil n\rceil^3 + 6n^2(\log n)^3)(5/n + 7/\log n)$$

is $o(n^r)$? Explain.

**(5)** Find the set of integer solutions to the system of congruences $x \equiv 4 \pmod 7$ and $x \equiv 6 \pmod{13}$.

**(6)** Prove by induction that $2^n > 10n$ holds for sufficiently large positive integers $n$.

**(7)** Prove that $\sqrt{6}$ is irrational.

**(8)** Prove or disprove the following statement: if $f$ is an injective function from $A$ to $B$, and $g$ is a surjective function from $B$ to $C$, then $g \circ f$ is a bijective function from $A$ to $C$.

This is the end! At this point, you may want to look over this sheet to make sure you have not omitted any problems.

Math 55, Fall 2001, Bjorn Poonen

Math 55 Practice Midterm Solutions (prepared by Nick Meyer)

1a. FALSE. There is a one-to-one correspondence between the half-open interval $H = [0, 1) \subset \mathbb{R}$ and the circle $C \subset \mathbb{R}^2$; this correspondence can be demonstrated by the bijective function $f : H \to C$ that sets $f(x) = (\cos 2\pi x, \sin 2\pi x)$ for $x \in H$. Since $H$ is a nonempty interval of the real numbers, it is uncountable; since $C$ is in one-to-one correspondence with $H$, it must also be.

1b. TRUE. The two statements are contrapositives of each other, hence logically equivalent.

1c. FALSE. Let $p = 23$; there is no prime $q$ strictly between $p$ and $p + 6 = 29$. (Note: there is nothing special about 6 here. For any positive $n$, we have that $2, 3, 4, \ldots, n$ all divide $n!$; hence $2|(n! + 2), 3|(n! + 3), \ldots, n|(n! + n)$. We thus have constructed a sequence of $n - 1$ consecutive composite numbers – namely, $n! + 2$ through $n! + n$.)

1d. TRUE. $30 = 2 \times 3 \times 5; 77 = 7 \times 11$. We must merely find an $m$ which does not have any of $2, 3, 5, 7, 11$ as a factor. 13 naturally suggests itself.

1e. FALSE. Indeed, everyone knows how Bob encrypted his message. To encrypt message $M$, Bob calculates ciphertext $C = M^e \textbf{ mod } n$ and sends $C$ to Alice. $n$ and $e$ comprise Alice's "public key"; as the name suggests, they are public information.

1f. TRUE. By Fermat's Little Theorem, $3^6 \equiv 1 \pmod 7$. Hence $3^{405} = ((3^{67})^6)(3^3) \equiv 3^3 \equiv 27 \equiv 13 \pmod 7$. (The last congruence follows because $7|(27 - 13)$; equivalently, $27 \textbf{ mod } 7 = 13 \textbf{ mod } 7 = 6$.

1g. FALSE. If $p$ is false and $q$ is true, then both $\neg p$ and $p \to q$ are true, but $\neg q$ is not.

2. It is easy to construct such a compound proposition in disjunctive normal form (see Section 1.2, Exercise 26). $(p \wedge \neg q \wedge \neg 4) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$ will do nicely.

3. $S$ consists of all positive even integers, and also the numbers $1, 3, 5, 7$. Hence 107 is not in $S$. Proof: Rules 1 and 3 together tell us that $1, 3, 5, 7$ are all in $S$. Rule 2 says that $a * 10^k$ is in $S$, for $a = 1, 3, 5, 7$ and $k$ any positive integer. These numbers can become arbitrarily large, and are all even. Rule 3 now implies that all positive even numbers are in $S$. Multiplying an even number by ten yields an even number, so applying Rule 2 gives us nothing new; we're done.

4. The given expression is $o(n^r)$ for all real $r \geq 3$. To prove this, we first recall that $\log n$ is $o(n^k)$ for any $k > 0$, and equivalently that $(\log n)^l$ is o(n) for any $l > 0$. Now we note that $4(\lceil n \rceil)^3 < 4(n+1)^3$, so is certainly $O(n^3)$; however, since it's equal to $4n^3$ for integer $n$, it's certainly not $o(n^3)$. By our above recollection, $6n^2(\log n)^3$ is $o(n^3)$. Thus the first term in the given expression is $O(n^3)$ (though not $o(n^3)$). Let us examine the second term. $5/n$ is $O(n^{-1}$; $7/\log n$ is $o(n^0)$, but – again, by our above recollection – it isn't $O(n^k)$ for any $k < 0$. Thus the second term is $o(n^0)$. The entire expression is $o(n^3 * n^0) = o(n^3)$, but not $o(n^k)$ for any $k < 3$.

5. Using the notation of Theorem 4, Section 2.5, we have: $m = 91, m_1 = 7, m_2 = 13, a_1 = 4, a_2 = 6$. Thus $M_1 = m/m_1 = 13$ and $M_2 = m/m_2 = 7$. $13y_1 \equiv 1 \pmod 7 \leftrightarrow -y_1 \equiv 1 \pmod 7$, so $y_1$ can be $-1$. $7y_2 \equiv 1 \pmod{13}$; $y_2 = 2$ is an obvious solution. Thus $x = a_1M_1y_1 + a_2M_2y_2 = -52 + 84 = 32$ is a solution to the system of congruences; the general solution is all integers $x$ such that $x \equiv 32 \pmod{91}$.

Alternatively, we can find $M_1$ and $M_2$ as above, and then posit that $x = aM_1 + bM_2$ for some coefficients $a, b$. Plugging this back into the original system of congruences allows us to find suitable $a, b$ and leads us quickly to the same solution we got above.

6. Claim: $2^n > 10n$ for all $n \geq 6$.

We prove this by induction on $n$. The base case is $n = 6$, and indeed $2^6 = 64 > 10 \times 6 = 60$. Now, if $2^n > 10n$, then $2^{n+1} = 2(2^n) > 2(10n) > 10(n + 1)$, with the last inequality holding as long as $n > 1$ (so it certainly holds when $n \geq 6$). This suffices to prove the inductive step, so we're done.

7. Claim: $\sqrt{6}$ is irrational.

We prove this by contradiction. Assume $\sqrt{6}$ is rational; then it can be expressed as $a/b$, where $a$ and $b$ are integers sharing no common factor larger than one. Then $6 = a^2/b^2$, so $a^2 = 6b^2$. Well, $2|6b^2$, so $2|a^2$, so we must have $2|a$. But this means that $4|a^2$, which means that $4|6b^2$, which implies that $2|b^2$, which means that $2|b$. Thus $a$ and $b$ have the common factor of 2; we have a contradiction! Thus our initial assumption is false, and we're done.

8. This statement is false. Let $A, B, C$ all be $\mathbb{Z}$, the set of integers. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = 2x$ (this is injective, but not surjective); let $g : \mathbb{Z} \to \mathbb{Z}$ be defined by $g(x) = x$ (this is bijective, so is certainly surjective). Then $(g \circ f)(x) = 2x$, so $g \circ f$ is not surjective.