Prof. Bjorn Poonen
October 16, 2001

MATH 55 MIDTERM SOLUTIONS (white)

(1) *(5 pts. each) 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 value of (-141) **mod** 8 *is* -5.
FALSE. The value of (-141) **mod** 8 is an integer between 0 and 7.

(b) The function $3n^2 \log n + 5n(\log n)^4$ *is* $O(n^3)$.
TRUE. If $c > 0$, then $\log n$ is $O(n^c)$, so $3n^2 \log n$ is $O(n^{2+c})$ and $5n(\log n)^4$ is $O(n^{1+4c})$. Thus $3n^2 \log n + 5n(\log n)^4$ is $O(\max\{n^{2+c}, n^{1+4c}\})$ for any $c > 0$. In particular, this holds for $c = 1/2$, in which case we find that $3n^2 \log n + 5n(\log n)^4$ is $O(n^3)$.

(c) The ceiling function $f(x) = \lceil x \rceil$, *considered as a function from* $\mathbb{R}$ *to* $\mathbb{R}$, *has an inverse function.*
FALSE. The ceiling function is not injective since $\lceil 1 \rceil = \lceil 1/2 \rceil$, so it is definitely not bijective. Hence it has no inverse function.

(d) The set $\{1, 2, 3\} \times \mathbb{Z}$ *is countable.*
TRUE. One can list its elements in a sequence as follows:

$$(1,0), (2,0), (3,0), (1,1), (2,1), (3,1), (1,-1), (2,-1), (3,-1), (1,2), (2,2), (3,2), (1,-2), \ldots$$

(e) The proposition $\forall x \exists y (x \leq y)$ *is true, when the universe of discourse is the set of natural numbers.*
TRUE. In words, this says "For all natural numbers x, there exists a natural number y that is at least as large as x." Here's a proof: Suppose x is a natural number. Then there exists a natural number y such that $x \leq y$, for instance $y = x$ itself.

(f) The numbers $35, 36, 37$ *are pairwise relatively prime.*
TRUE. Their factorizations are

$$35 = 5 \cdot 7, \qquad 36 = 2^2 \cdot 3^2, \qquad 37 = 37,$$

so no prime appears in two or more of these numbers.
Alternatively, use the Euclidean algorithm to check that

$$\gcd(35, 36) = 1, \qquad \gcd(35, 37) = 1, \qquad \gcd(36, 37) = 1.$$

(g) There are infinitely many integers x *satisfying both* $x \equiv 22 \pmod{99}$ *and* $x \equiv 25 \pmod{100}$. *(Hint: you don't need to solve this system.)*
TRUE. Since $\gcd(99, 100) = 1$, the Chinese Remainder Theorem applies, and says that there is a unique solution modulo 9900. This means that there is a solution b and that $b + 9900k$ is a solution for any $k \in \mathbb{Z}$, so there are infinitely many solutions.

(2) *(7 pts.) Find the hexadecimal (base 16) expansion of* $(270)_{10}$. *(Show your work.)*

Divide by 16:

$$270 = 16 \cdot 16 + 14.$$

The hexadecimal expansion of 270 equals the hexadecimal expansion of 16 with the "digit" $E = 14$ attached at the end. But $16 = (10)_{16}$, so $270 = (10E)_{16}$.

(3) *(15 pts.) Find* **two** *integer solutions to the congruence* $31x \equiv 2 \pmod{100}$. *(Explain how you are solving the problem as you go along.)*

First run the Euclidean algorithm on 31 and 100:

$$\begin{aligned} 100 &= 3 \cdot 31 + 7 \\ 31 &= 4 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 \cdot 1. \end{aligned}$$

Thus $\gcd(100, 31) = 1$, and working backwards we can express 1 as an integer linear combination of 100 and 31:

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - 2(31 - 4 \cdot 7) \\ &= 9 \cdot 7 - 2(31) \\ &= 9(100 - 3 \cdot 31) - 2(31) \\ &= 9(100) - 29(31). \end{aligned}$$

Thus

$$(-29)(31) \equiv 1 \pmod{100};$$

in other words, -29 is an inverse of 31 modulo 100. The original congruence is then equivalent to

$$(-29)31x \equiv (-29)2 \pmod{100},$$

which is equivalent to

$$x \equiv -58 \pmod{100}.$$

Thus -58 is a solution, and we can get other solutions by adding multiples of 100. In particular -58 and 42 are solutions. (These can be checked by plugging these into the original congruence.)

(4) *(10 pts.) Find the prime factorization of* 565. *(Explain how you are solving this problem. If you claim that a number is prime, explain why.)*

Begin trial division: 565 is not divisible by 2 or 3 but it is divisble by 5. In fact $565 = 5 \cdot 113$. Now we continue the trial division on 113, starting with the test whether it is divisible by 5. It is not divisible by 5, not divisble by 7, and the next prime 11 is greater than $\sqrt{113}$, so 113 must be prime. Thus the desired factorization is $565 = 5 \cdot 113$.

(5) *(8 pts.) Is the compound proposition* $(p \to q) \wedge (q \to r)$ *logically equivalent to* $p \to r$*? Explain.*

NO. Suppose p is F, q is T, and r is F. Then $q \to r$ is F, so $(p \to q) \wedge (q \to r)$ is F. On the other hand, $p \to r$ is T. (A more systematic way to do the problem is to write down the truth table for both compound propositions and observe that they do not always have the same truth value.) NOTE: It *is* true that $(p \to q) \wedge (q \to r)$ *implies* $p \to r$: this is what is behind the rule of inference called "hypothetical syllogism." But it is not true that $p \to r$ implies $(p \to q) \wedge (q \to r)$.

(6) *(15 pts.) Suppose that* f *is an injective function from the set* A *to the set* B*, and that* S *is a subset of* A*. Prove that* $f^{-1}(f(S)) = S$*. (Recall that "injective" means the same thing as "one-to-one", and recall that for* $T \subseteq B$*,* $f^{-1}(T)$ *is defined as* $\{ x \in A : f(x) \in T \}$*.)*

We first show that $f^{-1}(f(S)) \subseteq S$. Suppose $x \in f^{-1}(f(S))$. By definition of inverse image, this means that $f(x) \in f(S)$. By definition of $f(S)$, this means that $f(x) = f(a)$ for some $a \in S$. Since f is injective, $f(x) = f(a)$ implies that $x = a$. Since $a \in S$, we have $x \in S$. In other words, any element x of $f^{-1}(f(S))$ also belongs to S, so $f^{-1}(f(S)) \subseteq S$.

Next we show that $S \subseteq f^{-1}(f(S))$. Suppose that $x \in S$. Then $f(x) \in f(S)$, by definition of $f(S)$. Since f maps x into $f(S)$, it follows by definition of inverse image that $x \in f^{-1}(f(S))$. Thus $S \subseteq f^{-1}(f(S))$.

Since each of S and $f^{-1}(f(S))$ is a subset of the other, they are equal.

(7) *(10 pts.) The sequence* $a_0, a_1, a_2, \ldots$ *is defined recursively by* $a_0 = 1$ *and* $a_{n+1} = 3a_n - 1$ *for* $n \geq 0$*. Prove that* $a_n = (3^n + 1)/2$ *for all integers* $n \geq 0$*.*

We will prove the statement by induction on n. The base case, $n = 0$, holds, since $a_0 = 1$ and $(3^0 + 1)/2 = (1 + 1)/2 = 1$.

Now for the inductive step. Suppose that $n \geq 0$, and that $a_n = (3^n + 1)/2$ is known. Then

$$a_{n+1} = 3a_n - 1 = 3\left(\frac{3^n + 1}{2}\right) - 1 = \frac{3 \cdot 3^n + 3 - 2}{2} = \frac{3^{n+1} + 1}{2},$$

as desired.

Prof. Bjorn Poonen
October 16, 2001

MATH 55 MIDTERM SOLUTIONS (yellow)

(1) *(5 pts. each) 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 set $\{0,1\}^*$ of bit strings of finite length is a countable set.

TRUE, because one can list all the bit strings in a sequence, by listing all bit strings of length zero, then all of length one, and so on:

$$\lambda, 0, 1, 00, 01, 10, 11, \ldots$$

Alternatively, $\{0,1\}^*$ can be viewed as a subset of the set of all finite strings of typewriter symbols, which was shown in class to be countable.

(b) The proposition $\exists x \forall y (x \geq y)$ is true, when the universe of discourse is the set of natural numbers.

FALSE. In words, this says "There is a natural number x that is greater than or equal to all natural numbers y," which is false.

Alternatively, we can prove the negation, $\forall x \exists y (x < y)$, as follows. Suppose that x is a natural number. Then there exists a natural number y such that $x < y$, namely $y = x + 1$.

(c) The numbers $34, 35, 36$ are pairwise relatively prime.

FALSE, because $\gcd(34, 36) = 2$.

(d) There are infinitely many integers x satisfying both $x \equiv 12 \pmod{99}$ and $x \equiv 16 \pmod{100}$. (Hint: you don't need to solve this system.)

TRUE. Since $\gcd(99, 100) = 1$, the Chinese Remainder Theorem applies, and says that there is a unique solution modulo 9900. This means that there is a solution b and that $b + 9900k$ is a solution for any $k \in \mathbb{Z}$, so there are infinitely many solutions.

(e) The function $3n^2 \log n + 5n(\log n)^4$ is $O(n^3)$.

TRUE. If $c > 0$, then $\log n$ is $O(n^c)$, so $3n^2 \log n$ is $O(n^{2+c})$ and $5n(\log n)^4$ is $O(n^{1+4c})$. Thus $3n^2 \log n + 5n(\log n)^4$ is $O(\max\{n^{2+c}, n^{1+4c}\})$ for any $c > 0$. In particular, this holds for $c = 1/2$, in which case we find that $3n^2 \log n + 5n(\log n)^4$ is $O(n^3)$.

(f) The floor function $f(x) = \lfloor x \rfloor$, considered as a function from $\mathbb{R}$ to $\mathbb{R}$, has an inverse function.

FALSE. The floor function is not injective since $\lfloor 0 \rfloor = \lfloor 1/2 \rfloor$, so it is definitely not bijective. Hence it has no inverse function.

*(g) The value of (-133) **mod** 9 is -7.*

FALSE. The value of (-133) **mod** 9 is an integer between 0 and 8.

(2) *(8 pts.) Is the compound proposition* $(p \to q) \wedge (q \to r)$ *logically equivalent to* $p \to r$*? Explain.*

NO. Suppose p is F, q is T, and r is F. Then $q \to r$ is F, so $(p \to q) \wedge (q \to r)$ is F. On the other hand, $p \to r$ is T. (A more systematic way to do the problem is to write down the truth table for both compound propositions and observe that they do not always have the same truth value.) NOTE: It *is* true that $(p \to q) \wedge (q \to r)$ *implies* $p \to r$: this is what is behind the rule of inference called "hypothetical syllogism." But it is not true that $p \to r$ implies $(p \to q) \wedge (q \to r)$.

(3) *(10 pts.) Find the prime factorization of* 539*. (Explain how you are solving this problem. If you claim that a number is prime, explain why.)*

Begin trial division: 539 is not divisible by 2, 3, 5, but is divisible by the next prime, 7. In fact $539 = 7 \cdot 77$. Now we continue the trial division on 77, starting with the test whether it is divisible by 7; it is: $77 = 7 \cdot 11$. Now 11 is prime, since it has no divisors less than $\sqrt{11} < 4$. Thus the desired factorization is $539 = 7^2 \cdot 11$.

(4) *(7 pts.) Find the hexadecimal (base* 16*) expansion of* $(269)_{10}$*. (Show your work.)*

Divide by 16:

$$269 = 16 \cdot 16 + 13.$$

The hexadecimal expansion of 269 equals the hexadecimal expansion of 16 with the "digit" $D = 13$ attached at the end. But $16 = (10)_{16}$, so $269 = (10D)_{16}$.

(5) *(15 pts.) Find* ***two*** *integer solutions to the congruence* $31x \equiv 4 \pmod{100}$*. (Explain how you are solving the problem as you go along.)*

First run the Euclidean algorithm on 31 and 100:

$$\begin{aligned} 100 &= 3 \cdot 31 + 7 \\ 31 &= 4 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 \cdot 1. \end{aligned}$$

Thus $\gcd(100, 31) = 1$, and working backwards we can express 1 as an integer linear combination of 100 and 31:

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - 2(31 - 4 \cdot 7) \\ &= 9 \cdot 7 - 2(31) \\ &= 9(100 - 3 \cdot 31) - 2(31) \\ &= 9(100) - 29(31). \end{aligned}$$

Thus

$$(-29)(31) \equiv 1 \pmod{100};$$

in other words, -29 is an inverse of 31 modulo 100. The original congruence is then equivalent to

$$(-29)31x \equiv (-29)4 \pmod{100},$$

which is equivalent to

$$x \equiv -16 \pmod{100}.$$

Thus -16 is a solution, and we can get other solutions by adding multiples of 100. In particular -16 and 84 are solutions. (These can be checked by plugging these into the original congruence.)

(6) *(10 pts.) The sequence $a_0, a_1, a_2, \ldots$ is defined recursively by $a_0 = 1$ and $a_{n+1} = 3a_n - 1$ for $n \geq 0$. Prove that $a_n = (3^n + 1)/2$ for all integers $n \geq 0$.*

We will prove the statement by induction on n. The base case, $n = 0$, holds, since $a_0 = 1$ and $(3^0 + 1)/2 = (1 + 1)/2 = 1$.

Now for the inductive step. Suppose that $n \geq 0$, and that $a_n = (3^n + 1)/2$ is known. Then

$$a_{n+1} = 3a_n - 1 = 3\left(\frac{3^n + 1}{2}\right) - 1 = \frac{3 \cdot 3^n + 3 - 2}{2} = \frac{3^{n+1} + 1}{2},$$

as desired.

(7) *(15 pts.) Suppose that f is a surjective function from the set A to the set B, and that S is a subset of B. Prove that $f(f^{-1}(S)) = S$. (Recall that "surjective" means the same thing as "onto", and recall that $f^{-1}(S)$ is defined as $\{ x \in A : f(x) \in S \}$.)*

We first show that $f(f^{-1}(S)) \subseteq S$. Suppose $x \in f(f^{-1}(S))$. By definition of image, $x = f(y)$ for some $y \in f^{-1}(S)$. By definition of $f^{-1}(S)$, we have $f(y) \in S$. Thus $x \in S$. In other words, any element x of $f(f^{-1}(S))$ also belongs to S, so $f(f^{-1}(S)) \subseteq S$.

Next we show that $S \subseteq f(f^{-1}(S))$. Suppose that $x \in S$. Since f is surjective, there exists $a \in A$ such that $f(a) = x$. By definition of $f^{-1}(S)$, we have $a \in f^{-1}(S)$. Since $x = f(a)$, we then have $x \in f(f^{-1}(S))$. Thus $S \subseteq f(f^{-1}(S))$.

Since each of S and $f(f^{-1}(S))$ is a subset of the other, they are equal.