CSE 20, Discrete Mathematics, Spring, 1997
Relations, Equivalence Relations and Partial Orders
(Chapter 10)
Homework 4, Due. May 29.
Answer Key, Selected problems.

Short answers (2 points each):

a. Find an integer x so that $x23 \equiv_{32} 1$, i.e., $32|23x - 1$.

We go through the Euclidean algorithm . 9=32-23; 5=23-2*9; 4=9-5; 1=5-4. Then we reverse to get 1=5-4= 2*5-9= 2*23-5*9=7*23-5*32. Thus, $7 * 23 \equiv_{32} 1$. b. In New Hampshire, which has no sales tax, pencils cost 32 cents each and erasers cost 23 cents each. I spent a total of \$5.08 on pencils and erasers. How many pencils did I buy?

Let a be the number of pencils and b the number of erasers. We know $a32+b23 = 508$. Taking both sides modulo 32, we know $b*23 \equiv_3 2508 \equiv_{32} 508 mod 32 = 28 \equiv_{32} -4$. So then $b \equiv_{32} b * 1 \equiv_{32} b * 23 * 7 \equiv_{32} -4 * 7 \equiv_{32} -28 \equiv_{32} 4$. Now a, b are positive integers, so the only possible value is $b = 4$, since otherwise $b \geq 36$ and a will be negative. Then $32a = 508 - 4(23) = 416$, so $a = 13$.

Compute the remainder when $1,000,000,000,000,000,000,000,000,000,000 = 10^{30}$ is divided by 13.

Use the method of repeated squaring: $10^2 \equiv_{13} 100 \equiv_{13} 9 \equiv_{13} -4$; $10^4 \equiv_{13} -4^2 = 16 \equiv_{13} 3$ $10^8 \equiv_{13} 3^2 \equiv_{13} 9 \equiv_{13} -4$; $10^16 = 4^2 \equiv_{13} 3$; $10^24 = 10^16 * 10^8 \equiv_{13} 3 * (-4) \equiv_1 31$; $10^{28} = 10^24 * 10^4 \equiv_{13} 1 * 3 = 3$ $10^{30} = 10^{28} * 10^2 \equiv_{13} 3 * -4 \equiv_{13} 1$.

Full Proofs (5pts. each):

Prefix partial order Let $S = \{0, 1\}^*$ be the set of all binary words . Let xPy be the prefix relationship, i.e., xPy if and only if there is an $w \in S$ with $y = x \circ w$, where $\circ$ is the concatenation of two strings. Prove that P is a partial order. You may use the following without proof: $x = x \circ \lambda$, where λ represents the empty word (the only word of length 0); $l(x \circ a) = l(x) + l(a)$, where $l(x)$ is the (non-negative integer) length of the word, and $(x \circ a) \circ b = x \circ (a \circ b)$.

Proof: We must prove that P is reflexive, transitive, and anti-symmetric.

To see that P is reflexive, let $x \in S$. Then $x = x \circ \lambda$, so xPx (applying the definition of P with $w = \lambda$.) Thus, P is reflexive.

To see that P is transitive, let $x, y, z \in S$ and assume xPy and yPz. Then there are w_1, w_2 so that $y = x \circ w_1$ and $z = y \circ w_2$, so $z = (x \circ w_1) \circ w_2 = x \circ (w_1 \circ w_2)$. So (picking $w = w_1 \circ w_2$ in the definition of P) xPz. Thus, P is transitive.

To see that P is anti-symmetric. let $x, y \in S$ and assume xPy and yPx. Then there are w_1, w_2 so that $y = x \circ w_1$ and $x = y \circ w_2$. Then $x = x \circ w_1 \circ w_2$, and $l(x) = l(x) + l(w_1) + l(w_2)$. Thus, $l(w_1) = l(w_2) = 0$, and $w_1 = w_2 = \lambda$, the only string of length 0. Thus $y = x \circ \lambda = x$. Therefore, P is anti-symmetric.

Section 10.2. pp. 554-555 20, 35 20. $xPy \iff \exists p(p$ is prime and $p|x \wedge p|y$. Is P reflexive? No, because 1 has no prime factors, so $\neg 1P1$. (To be reflexive we must have xPx for all x. One counter-example hence suffices.) Is P symmetric. Yes. If xPy there is a prime number p so that $p|x$ and $p|y$. Then $p|y$ and $p|x$, so yPx. Is P transitive? No. Let $x = 2, y = 6, z = 3$. Then xPy since they share the prime factor 2, and yPz since they share the factor 3, but $\neg xPz$.

35. The relationship of being parallel lines is reflexive for this problem, because you are told for the purposes of this promblem that a line is parallel to itself. It is symmetric since if one line is parallel to another , than the second is parallel to the first. It is also transitive, since if one line is parallel to a second and the second is parallel to the third, then all three have the same slope, and the first is parallel to the third.

Section 10.3, pp. 571-572 31 Assume for a fixed equivalence relation R, that $a \in [b] = \{c|cRb\}$. Prove $[a] = [b]$.

By the definition of [b], aRb.

Let $c \in [a]$ Then cRa by definition of $[a]$. cRb by symmetry. So $c \in [b]$. Thus $[a] \subseteq [b]$, and

Let $c \in [b]$ Then cRb by definition of $[b]$. bRc by symmetry. and then aRc by transitivity (since aRb), so cRa by symmetry. So $c \in [a]$. Thus $[b] \subseteq [a]$

Thus, since $[a] \subseteq [b]$ and $[b] \subseteq [a]$, $[a] = [b]$. 37 Assume R is symmetric and transitive, and that $\forall x \exists y xRy$ Prove R is reflexive.

Let x be any element of the domain. Then there is a y so that xRy. Since R is symmetric, yRx. By transitivity, since xRy and yRx, xRx. Since xRx for an arbitrary element of the domain, R is reflexive.

Let R be the following relation on $Z \times Z$ defined by $(a, b)R(c, d)$ if and only if $a \leq c$ and $b \leq d$. Prove that R is a partial order. Does R have an infinite chain? An infinite anti-chain?

Let (a, b) be any point. Then $a \leq a$ and $b \leq b$, so $(a, b)R(a, b)$. Thus, R is reflexive.

Assume $(a, b)R(c, d)$ and $(c, d)R(a, b)$ Then $a \leq c, b \leq d, c \leq a$ and $d \leq b$.

Thus $a = c$ and $b = d$, so $(a.b) = (c, d)$. Thus, R is anti-symmetric.

. Assume $(a, b)R(c, d)$ and $(c, d)R(e, f)$ Then $a \leq c, b \leq dc \leq e$ and $e \leq f$. Thus $a \leq e$ and $b \leq f$, so $(a, b)R(e, f)$. Thus R is transitive.

Since R is reflexive, anti-symmetric and transitive, it is a partial order.

An infinite chain in R is the sequence $(1,1)R(2,2)R...R(x,x)R....$ An infinite anti-chain for R is the set $\{(1,-1),(2,-2),...(n,-n),...\}$.

Let R be the relation on $Z \times Z$ defined by $(a,b)R(c,d)$ if and only if $a+b=c+d$. Prove that R is an equivalence relation. What are R's equivalence classes?

R is reflexive, since $a+b=a+b$,so $(a,b)R(c,d)$. R is symmetric, since if $(a,b)R(c,d)$, $a+b=c+d=a+b$, so $(c,d)R(a,b)$. R is transitive, since if $(a,b)R(c,d)$ and $(c,d)R(e,f)$, $a+b=c+d=e+f$, so $(a,b)R(e,f)$. Thus, R is an equivalence relation. For each integer k let $C_k=\{(a,b)|a+b=k\}$. The classes C_k for all integers k are the equivalence classes for R.

Let p be a prime and let $0 \leq a < p$. Prove that there are at most two numbers $x, 0 \leq x < p$ so that $x^2 mod p = a$.

Assume $x_1^2 \equiv_p x_2^2 \equiv x_3^2$, for some $0 \leq x_1 < x_2 < x_3 \leq p-1$. Then $x_1^2 - x_2^2 mod p = (x_1^2 mod p - x_2^2 mod p) mod p = 0 mod p = 0$. In other words, p evenly divides $x_1^2 - x_2^2$. Now $x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2)$, so since if a prime number divides a product, then it divides one of the factors, either p divides $x_1 - x_2$ or p divides $x_1 + x + 2$. But the first case is impossible, since $1 \leq x_2 - x_1 \leq (p-1) < p$. So the second case must hold. Since $1 \leq x_1 + x_2 \leq 2(p-1) < 2p$, the only multiple of p that could equal $x_1 + x_2$ is p, so $x_1 + x_2 = p$.

By a similar argument, $x_1 + x_3 = p$. But then $x_2 = x_3 = p - x_1$, a contradiction. Thus, there cannot be three such integers whose square mod p is a, so there are at most 2. On the domain $\{1,,p\}$, the above proof hints at a reason f is not 1-1. Namely, if $p|(a+b)$, then $a^2 mod p = b^2 mod p$. Thus, picking $b = p - a$ for $a \in \{1,..(p-1)/2\}$ gives us a distinct pair whose squares have the same remainder mod p. This is the equivalent of $x^2 = (-x)^2$ over the real numbers. For example, $a = 1, b = p-1$, we have $a^2 mod p = 1 mod p = 1 = p^2 - 2p + 1 mod p = b^2 mod p$. If p is a composite number, we might have that p divides $a^2 - b^2$ without dividing $a - b$ or $a + b$. For example, $p = 15, a = 4, b = 1$, we have $a - b = 3$ and $a + b = 5$, so p divides neither, but does divide their product. So $1^2 mod 15 = 1 = 16 mod 15 = 4^2 mod 15$.

Extra Credit problem (2 points extra credit .) 1. There are 26 people in a line to get into a theater. Prove that there are 6 people that are either in increasing or decreasing order of height from front to back.