Split "P" Soup
Solutions to Locker Problems and Assorted Appetizers
Greg Martin and Emmanuel Knafo
SIMMER (Fields Institute)—May 4, 2000

1. *Locker chaos.* Let's focus on a particular locker, say locker #20. The first student opens the locker, the second student closes it, the fourth student opens it, the fifth student closes it, the tenth student opens it, and the twentieth student closes it for good. The students that change the locker correspond exactly to the divisors of 20 (1, 2, 4, 5, 10, and 20), and we can see that this will always be the case—the dth student that touch the mth locker exactly when m is a multiple of d, or equivalently, d is a divisor of m.

   To decide which lockers are open at the end of the day, we need to figure out which lockers are changed by an *odd* number of students; in other words, we need to decide which numbers m have an odd number of divisors. If we start working out the problem by hand, we see that of the first ten lockers the ones that are open at the end are #1, #4, and #9, while the rest are closed at the end. This leads to the following guess: the lockers that are open at the end are precisely the lockers numbered with a square! To prove this, we need to show that a number m has an odd number of divisors if and only if m is a square.

   "Odd" means "congruent to 1 modulo 2", so instead of counting the divisors, let's just think of what the number of divisors is modulo 2. If d is a divisor of m satisfying the inequality $d < \sqrt{m}$, then m/d is also a divisor of m, and $m/d > \sqrt{m}$. Therefore these divisors come in pairs: each divisor less than $\sqrt{m}$ is paired with one exceeding $\sqrt{m}$ (and vice versa, of course). Since we only care about the number of divisors modulo 2, a pair of divisors is equivalent to no divisors, and we can forget all these divisors.

   Well, if we forget all divisors of m that are less than $\sqrt{m}$, and also all those that are greater than $\sqrt{m}$, there aren't going to be many left, are there? In fact, if m is a square, say $m = k^2$, then there is exactly *one* divisor, namely k, left after pairing the others off; in this case, the total number of divisors is congruent to *one* modulo 2, which shows that squares have an odd number of divisors. On the other hand, if m is not a square, then there are *no* divisors that haven't been paired off; in this case, the total number of divisors is congruent to *zero* modulo 2, which shows that non-squares have an even number of divisors. So we've proved that our guess is correct!

   Another way to show the same fact is to prove a formula for the number of divisors of a number m: if the prime factorization of m is $p_1^{r_1} \times p_2^{r_2} \times \cdots \times p_j^{r_j}$, then the number of divisors of m is exactly $(r_1 + 1)(r_2 + 1) \ldots (r_j + 1)$. This number is odd if and only if each factor is odd (put another way, the product of the numbers $r_i + 1$ is not a multiple of the prime 2 if and only if none of the numbers $r_i + 1$ is a multiple of 2). For each factor to be odd, we need each r_i to be even, say $r_i = 2s_i$; and then m is indeed a square:

$$m = \left(p_1^{s_1} p_2^{s_2} \ldots p_j^{s_j} \right)^2.$$

   This second technique can also answer questions such as the following: *Which numbers have the property that the sum of all of their divisors is odd?*

2. *Rocks and lockers.* Again, by working through the beginning of the problem by hand, we see that the first few lockers to have rocks placed in them are 2, 3, 5, 7, and 11. This suggests the following guess: the lockers with rocks in them are precisely the prime numbers.

   Again, we switch perspectives: instead of thinking about one student at a time and the lockers he/she closes, we think about one locker at a time and the students who want that locker closed. The student who closes locker #m must have put a rock in some locker, say locker #d; and since this student is making sure that all lockers that are multiples of d are closed, we see that d must be a divisor of m. In fact, the student who actually closes locker #m (as opposed to merely seeing that it is already closed) must have put his/her rock in locker #d, where d is the *smallest* divisor of m other than 1 (since locker #1 started the day already closed).

So which lockers end up with rocks in them? Well, as we just discovered, locker #m gets a rock if and only if m equals d, where d is the smallest divisor of m other than 1. Of course, this is precisely the definition of a prime number reworded slightly. So our guess is correct here as well! (We sure are good guessers.) Since every student put a rock in some locker and every locker ended up closed, the number of students was therefore the number of primes between 1 and 100, or 25.

This problem describes a long-existing method for calculating primes called the *Sieve of Eratosthenes*. Eratosthenes was a Greek scientist of the third century B.C. (when the Greek empire extended to present-day Libya, his birthplace) with many accomplishments in astronomy including a fairly accurate calculation of the circumference of the earth. He worked out this method for determining the primes up to some bound (we have used the bound 100, the number of lockers), and he noted that as soon as all numbers up to the square root of the bound have been dealt with, all the remaining numbers are automatically prime—there is no need to go through them one by one. This is because every composite number m has not just a prime factor, but indeed a prime factor $p \leq \sqrt{m}$. In our example, once the first four students put rocks in lockers #2, #3, #5, and #7 and close the corresponding lockers, all the lockers up to $\sqrt{100} = 10$ are then closed, and the lockers remaining open are already all primes.

3. *Counting change.* Let p, d, and q represent the number of pennies, dimes, and quarters, respectively. Since the total number of coins is 100, we immediately have the equation $p + d + q = 100$. If we want the total value of the coins to be \$5.00, this gives us the equation $p + 10d + 25q = 500$. Subtracting the first of these equations from the second eliminates the variable p, and the resulting equation is $9d + 24q = 400$.

But there are no solutions in integers to this equation! The slickest way to see this is by reducing modulo 3. We have $9 \equiv 24 \equiv 0 \pmod 3$ and $400 \equiv 1 \pmod 3$, so the equation $9d + 24q = 400$ implies the congruence $0d + 0q \equiv 1 \pmod 3$, which is impossible. Therefore there are no solutions to the \$5.00 version of the problem.

If instead we want the total value to be \$4.99, the second equation becomes $p + 10d + 25q = 499$, and subtracting the two equations gives $9d + 24q = 399$. Now everything in sight is divisible by 3, and when we divide by 3 we are left with the equation $3d + 8q = 133$.

To find solutions in integers to such a linear equation, we can again use congruences. If we look modulo 8, the q-term disappears, and we are left with the congruence $3d \equiv 133 \equiv 5 \pmod 8$. Multiplying both sides of this congruence by 3 yields $9d \equiv 15 \pmod 8$, which is the same as $d \equiv 7 \pmod 8$ after reducing once again the numbers modulo 8. Therefore it is necessary for d to be of the form $7 + 8k$ for some integer k, and we easily see that setting $q = (133 - 3(7 + 8k))/8 = 14 - 3k$ makes the equation $3d + 8q = 133$ satisfied. Going back to the first equation, we see that we must also set $p = 100 - (7 + 8k) - (14 - 3k) = 79 - 5k$.

We have found the entire set of solutions to the pair of equations $p + d + q = 100$, $p + 10d + 25q = 499$ in integers; for the solution to be in *nonnegative* integers, we need to restrict to values k such that the three quantities $7 + 8k$, $14 - 3k$, and $79 - 5k$ are all nonnegative. This restricts k to lie between $-7/8$ and $14/3$, i.e., $k = 0$, 1, 2, 3, or 4. We conclude that the five solutions to the \$4.99 version of the problem are

$$(p, d, q) = (79, 7, 14), (74, 15, 11), (69, 23, 8), (64, 31, 5), \text{ and } (59, 39, 2).$$

4. *Monkey business.* Let x represent the original number of coconuts in the original pile, and define $A = (n-1)/n$. After the first castaway goes back to sleep, there are $(x-1)A = Ax - A$ coconuts left in the pile. After the second castaway goes back to sleep, there are $(Ax - A - 1)A = A^2 x - (A^2 + A)$ coconuts left in the pile. Continuing in this way, we see that after the nth castaway goes back to sleep, there are

$$A^n x - (A^n + A^{n-1} + \cdots + A^2 + A) = A^n x - A\left(\frac{1 - A^n}{1 - A}\right)$$

coconuts left in the pile. Substituting in the value $A = (n-1)/n$ and rearranging terms, this gives

$$(n-1)^n \left(\frac{x + n - 1}{n^n}\right) - n + 1$$

coconuts left over. Since no coconut was ever split by the castaways, this quantity must be an integer. But n^n cannot have any factor in common with $(n-1)^n$, since no prime can divide the two consecutive integers $n-1$ and n; therefore n^n divides $x+n-1$. (This is why we've grouped the terms as we have.)

The next morning, the castaways realize that this amount is divisible by n. This means that we have the congruence

$$(n-1)^n\left(\frac{x+n-1}{n^n}\right) - n + 1 \equiv 0 \ (\text{mod } n),$$

or equivalently, since $n \equiv 0 \ (\text{mod } n)$,

$$\frac{x+n-1}{n^n} \equiv (-1)^{n+1} \ (\text{mod } n).$$

From the definition of congruences, we can check that if a/b is an integer and $a/b \equiv c \ (\text{mod } d)$, then $a \equiv bc \ (\text{mod } bd)$. (The converse is true as well.) Therefore we have

$$x + n - 1 \equiv (-1)^{n+1} n^n \ (\text{mod } n^{n+1}),$$

which tells us that

$$x \equiv (-1)^{n+1} n^n - n + 1 \ (\text{mod } n^{n+1}),$$

We conclude that all the possible solutions to the problem are given by

$$x = (-1)^{n+1} n^n - n + 1 + k n^{n+1},$$

where k is an integer such that the right-hand side is positive.

When n is odd, the smallest such x is obtained by putting $k=0$, giving $x = n^n - n + 1$. When n is even, the smallest such x is obtained by putting $k=1$, giving

$$x = -n^n - n + 1 + n^{n+1} = (n^n - 1)(n - 1).$$

For example, if there are 5 castaways then the smallest number of coconuts in the original pile is $5^5 - 4 = 3121$ coconuts. If there are 4 castaways then the smallest number of coconuts in the original pile is $(4^4 - 1)3 = 765$ coconuts.

The power of using congruences to solve this problem is really demonstrated when we generalize this problem to n castaways and r monkeys. Following the same method, we find without too many complications that the least amount of coconuts is $rn^n - r(n-1)$ when n is odd and $n^n(n-r) - r(n-1)$ when n is even. Try it and see!

Split "P" Soup
Strategies for the Modular Arithmetic Games
Greg Martin and Emmanuel Knafo
SIMMER (Fields Institute)—May 4, 2000

Here is the winning strategy for both of the modular arithmetic games, indicating how the player who chooses who goes first can win every time with perfect play: *If the modulus M is odd, tell the other player to go first. If the modulus M is even, choose to go first yourself.*

Although the winning strategy is the same in both cases, the reasons behind the strategy are much different for the two games. Before explaining why this is a good strategy in each case, notice that both games are easier to play if you always reduce the running total modulo M after every play, and just keep track of the reduced totals which lie between 0 and $M - 1$.

The Modular Addition Game. Although the game is phrased in terms of choosing an integer n and adding it to the running total T, one can easily arrange for the running total to become whatever you want: if the running total is T and you want it to become T', choose the integer $T' - T$ on your turn. Therefore, both players are essentially choosing numbers between 0 and $M - 1$ on their turns. Nobody wants to choose a number that has already been chosen, and nobody wants to choose 0; the player who finally runs out of good choices is the first player if M is odd and the second player if M is even. Thus the strategy here is "play not to lose".

The Modular Multiplication Game. If the modulus M is even, the player who starts wins easily and quickly by simply choosing $M/2$. If the other player multiplies by an even number on his/her turn, then the running total will be a multiple of M; on the other hand, if the other player multiplies by an odd number, then the running total will remain congruent to $M/2$ since

$$(2k + 1)M/2 = kM + M/2 \equiv M/2 \pmod{M},$$

which still results in a loss for the second player.

On the other hand, suppose that the modulus M is odd. At each stage, one can look at the greatest common divisor of the running total T and the modulus M. For instance, in the example game modulo 15 with the sequence of running totals 2, 12, 24, 216, 648, -3240, the corresponding sequence of "running gcd values" is 1, 3, 3, 3, 3, 15. It turns out that if T is the current running total and you want to make the new running total equal to T', then you can find an integer n such that $nT \equiv T' \pmod{M}$ if and only if $\gcd(T', M)$ is a multiple of $\gcd(T, M)$. (Check this!) In particular, the "running gcd value" can increase as the game goes along, but it can never decrease. Now we claim that the following "play not to lose" strategy is a sure win for the second player: *always choose an integer n such that the new running gcd value $\gcd(nT, M)$ is the same as the previous running gcd value $\gcd(T, M)$.*

We claim that if you follow this "play not to lose" strategy, you will never be forced into making the running gcd value increase, even if the opponent is also "playing not to lose". This is because, as it turns out, *for odd numbers M, the number of integers T between 0 and $M - 1$ such that $\gcd(T, M)$ takes a certain value is even.* The reason? Because $\gcd(M - T, M) = \gcd(-T, M) = \gcd(T, M)$ (check this too!), these integers can be paired off (like in the first solution to the "Locker chaos" problem). Therefore if the other player is the first to attain a particular gcd value (including at the very beginning of the game), you can always outlast him/her until he/she is forced to increase the running gcd value yet again. And if the other player is always increasing the running gcd value, he/she will be the one who finally makes $\gcd(T, M) = M$, which means that T is a multiple of M!

For both of these games, think about the following question: *If the other player decides who goes first, how can you take advantage of a mistake by the other player during play?* In the Modular Multiplication Game, a single mistake by the "player in control" will not necessarily make him/her lose unless the other player plays perfectly from then on.