MAT 3343, APPLIED ALGEBRA, FALL 2003

Answers to Problem Set 3 (due Oct. 10)

Problem 1 Suppose we want to encrypt "Applied Algebra", or 0116; 1612; 0905; 0400; 0112; 0705; 0218; 0100. Each message M is encoded as $C = M^e (\bmod 65)$. Exponentiation modulo 65 is easy to calculate by the method of repeated squaring, e.g. for $M = 116$, we have

$$\begin{array}{lllllll}
M & = & 116 & & & & \\
M^2 & = & 116^2 & = & 13456 & = & 1817 \quad (\bmod 11639) \\
M^4 & = & 13456^2 & = & 3301489 & = & 7652 \quad (\bmod 11639) \\
M^8 & = & 3301489^2 & = & 58553104 & = & 8934 \quad (\bmod 11639) \\
M^{16} & = & 58553104^2 & = & 79816356 & = & 7733 \quad (\bmod 11639) \\
M^{32} & = & 79816356^2 & = & 59799289 & = & 9746 \quad (\bmod 11639) \\
M^{64} & = & 59799289^2 & = & 94984516 & = & 10276 \quad (\bmod 11639) \\
M^{65} & = & 10276 \cdot 116 & = & 1192016 & = & 4838 \quad (\bmod 11639)
\end{array}$$

This method requires only about 8 digits of accuracy and can be done on a normal calculator. Of course, you could also calculate the exponentiation in a single step, and then reduce modulo 11639:

$$\begin{array}{lll}
116^{65} & = & 15479940952334433407499346181354052750689233887150719 9\\
& & 3157633632646686459619627534020027093470786693742622 85\\
& & 06952226048453504273062297 6\\
& = & 4838 (\bmod 11639)
\end{array}$$

However, this is more than most calculators can handle, and it is not very efficient computationally either.

The complete encryption of the above message is 4838; 5646; 6555; 8036; 2485; 10062; 6384; 11391.

Problem 2 We are given $x \in \mathbb{Z}_N$ such that $x^2 = x$, thus $x^2 - x = 0$, thus $x(x-1) = 0$ in $\mathbb{Z}_N$. This means that $N | x(x-1)$. On the other hand, $x \neq 0, 1$, so $N \not| x$ and $N \not| (x-1)$. Now consider $a = \gcd(N, x)$. Then $a | N$ and $a | x$ by definition of gcd. But we cannot have $a = 1$, or else N and x are relatively prime, and $N | (x-1)$ by Theorem 5(2), p.41. Also, we cannot have $a = N$, or else $N | x$. It follows that a is a non-trivial factor of N (and thus a prime factor, since $N = pq$ is a product of two primes).

Problem 3 The generalized Chinese Remainder Theorem: Let $n_1, \ldots, n_k$ be integers such that $\gcd(n_i, n_j) = 1$ for all $i \neq j$, and let $n = n_1 n_2 \cdots n_k$. Given integers $a_1, \ldots, a_k$, there exists a unique $a \in \mathbb{Z}_n$ such that $a \equiv a_i (\bmod n_i)$ for all $i = 1, \ldots, k$.

Proof. Existence: By induction on k. If $k = 1$, there is nothing to show, and if $k = 2$, this is just the ordinary Chinese Remainder Theorem. For $k > 2$, let $n' = n_1 n_2 \cdots n_{k-1}$. By induction hypothesis, we can find $a' \in \mathbb{Z}_{n'}$ such that $a' \equiv a_i (\bmod n_i)$ for all $i = 1, \ldots, k-1$. Now observe that $\gcd(n', n_k) = 1$, and use the ordinary Chinese Remainder Theorem to find $a \in Z_n$ such that $a \equiv a' (\bmod n')$ and $a \equiv a_k (\bmod n_k)$. Then $a \equiv a_i (\bmod n_i)$ for all $i = 1, \ldots, k$ as required.

Uniqueness: Suppose $a, a' \in \mathbb{Z}_n$ such that $a \equiv a_i (\bmod n_i)$ and $a' \equiv a_i (\bmod n_i)$ for all $i = 1, \ldots, k$. Then $a \equiv a' (\bmod n_i)$ for all i, hence $n_i | (a - a')$ for all i, hence $n_1 n_2 \cdots n_k | (a - a')$ (because all the n_i are relatively prime to each other, by repeated application of Theorem 5(1), p.41). Therefore $a \equiv a' (\bmod n)$, so $a = a'$ in $\mathbb{Z}_n$. □

Problem 4 (a) From the Chinese Remainder Theorem, we know that we can find elements $a_1, \ldots, a_8 \in \mathbb{Z}_N$ such that

$$\begin{array}{lll}
a_1 \equiv +1 (\bmod p) & a_1 \equiv +1 (\bmod q) & a_1 \equiv +1 (\bmod r) \\
a_2 \equiv +1 (\bmod p) & a_2 \equiv +1 (\bmod q) & a_2 \equiv -1 (\bmod r) \\
a_3 \equiv +1 (\bmod p) & a_3 \equiv -1 (\bmod q) & a_3 \equiv +1 (\bmod r) \\
a_4 \equiv +1 (\bmod p) & a_4 \equiv -1 (\bmod q) & a_4 \equiv -1 (\bmod r) \\
a_5 \equiv -1 (\bmod p) & a_5 \equiv +1 (\bmod q) & a_5 \equiv +1 (\bmod r) \\
a_6 \equiv -1 (\bmod p) & a_6 \equiv +1 (\bmod q) & a_6 \equiv -1 (\bmod r) \\
a_7 \equiv -1 (\bmod p) & a_7 \equiv -1 (\bmod q) & a_7 \equiv +1 (\bmod r) \\
a_8 \equiv -1 (\bmod p) & a_8 \equiv -1 (\bmod q) & a_8 \equiv -1 (\bmod r)
\end{array}$$

Clearly, each such element satisfies $a_i^2 \equiv 1$ modulo p, q, r, and thus modulo N; thus, each a_i is a square root of unity. On the other hand, any square root of unity b in $\mathbb{Z}_N$ must also be a square root of unity in $\mathbb{Z}_p$, $\mathbb{Z}_q$, and $\mathbb{Z}_r$, and must therefore satisfy $b \equiv \pm 1$ modulo p, q, r, and must thus be one of the a_i. Finally, all the a_i are different, since $+1 \neq -1$ modulo an odd prime. Therefore, there are precisely 8 square roots of unity.

(b) The Chinese Remainder Theorem, along with the equations in part (a), allows us to compute $a_1, \ldots, a_8$ efficiently.

(c) To compute this efficiently, we first compute the solutions x, y, z to the following equations:

$$\begin{array}{lll} x \equiv 1 (\mathrm{mod}\, 7) & x \equiv 0 (\mathrm{mod}\, 11) & x \equiv 0 (\mathrm{mod}\, 13) \\ y \equiv 0 (\mathrm{mod}\, 7) & y \equiv 1 (\mathrm{mod}\, 11) & y \equiv 0 (\mathrm{mod}\, 13) \\ z \equiv 0 (\mathrm{mod}\, 7) & z \equiv 0 (\mathrm{mod}\, 11) & z \equiv 1 (\mathrm{mod}\, 13) \end{array}$$

This can be done by Euclid's algorithm, and we find $x = -286$, $y = 364$, and $z = -77$. Then $a_1, \ldots, a_8$ can be rapidly computed in this basis:

$$\begin{array}{lclcr} a_1 & = & x+y+z & = & 1 \\ a_2 & = & x+y-z & = & 155 \\ a_3 & = & x-y+z & = & -727 \\ a_4 & = & x-y-z & = & -573 \\ a_5 & = & -x+y+z & = & 573 \\ a_6 & = & -x+y-z & = & 727 \\ a_7 & = & -x-y+z & = & -155 \\ a_8 & = & -x-y-z & = & -1 \end{array}$$

(d) Let x be a square root of unity in $\mathbb{Z}_N$ with $x \neq \pm 1$. Then $x^2 = 1$ in $\mathbb{Z}_N$, thus $N|(x-1)(x+1)$. Let $a = \gcd(x+1, N)$. Then $a|N$. We cannot have $a = 1$, or else $x+1$ and N are relatively prime, thus $N|(x-1)$, contradicting $x \neq 1 (\mathrm{mod}\, N)$. On the other hand, we cannot have $a = N$, or else $N|(x+1)$, contradicting $x \neq -1 (\mathrm{mod}\, N)$. Thus, a is a non-trivial factor of N. Since $N = pqr$ is the product of three primes, either a or N/a is prime, thus we have found one of the prime factors of N. We cannot do any better with the given information.

Problem 5 (a) This problem is most fun (and most realistic) if we actually pick random numbers $b \in \{1, \ldots, 118\}$ to do the test.

Random number:	Test:	Result:
$b = 74$	$b^{118} = 25 (\mathrm{mod}\, 119)$	fail

The test has already failed on our first random choice of b. Therefore, 119 is not prime. In order not to spoil our fun, we continue testing some more numbers:

Random number:	Test:	Result:
$b = 77$	$b^{118} = 21 (\mathrm{mod}\, 119)$	fail
$b = 109$	$b^{118} = 60 (\mathrm{mod}\, 119)$	fail
$b = 102$	$b^{118} = 102 (\mathrm{mod}\, 119)$	fail

As we can see, the probability of failing the test seems to be very much in our favor; indeed we did not find any b which passed the test.

(b) Again, we pick our candidates $b \in \{1, \ldots, 560\}$ at random. Note that $560 = 2^4 \cdot 35$. All calculations are modulo 560.

b (random)	b^{35}	b^{70}	b^{140}	b^{280}	b^{560}	Result:
344	353	67	1	1	1	fail
297	495	429	33	528	528	fail
300	243	144	540	441	375	fail
224	452	100	463	67	1	fail
468	219	276	441	375	375	fail
545	494	1	1	1	1	fail

Again, the test failed with the first random number we picked; we could have stopped right there. (We continued just for the fun of it). Again, the odds seemed to be heavily stacked in our favor, as we could not in fact find any b which passed the test in the first 6 trials.

Note that 3 of our 6 random number would have passed the Fermat pseudoprime test.