Math 55: Discrete Mathematics, Fall 2008
Homework 4 Solutions

3.7: 32. First of all, factor $1729 = 7 \cdot 13 \cdot 19$. Now notice that for each of the prime factors p, $p-1$ divides 1728. Hence if $x \not\equiv 0 \pmod{1729}$, then Fermat's theorem implies that $x^{1728} \equiv 1 \pmod 7$, $x^{1728} \equiv 1 \pmod{13}$, and $x^{1728} \equiv 1 \pmod{19}$. By the Chinese Remainder Theorem, it follows that $x^{1728} \equiv 1 \pmod{1729}$, that is, 1729 is a Carmichael number. [This problem was also done in lecture.]

46. The letter pairs are represented by the integers 120, 2001, 311. Encrypting these with $E(x) = x^{13} \pmod{2537}$, we get 286, 798, 425.

(A) The decryption exponent is $13^{-1} \pmod{42 \cdot 58}$, or $d = 937$. Computing $286^{937} \pmod{2537}$ gives back 120, as expected.

*60. The solutions are $x \equiv \pm 4, \pm 11, \pm 31, \pm 46 \pmod{105}$.

To find them, observe that modulo each prime, the solutions are $x \equiv \pm 4$. Thus $x \equiv \pm 1 \pmod 3$, $x \equiv \pm 1 \pmod 5$, $x \equiv \pm 3 \pmod 7$. For each of the eight possible combinations of signs, solve the three simultaneous congruences using the Chinese Remainder Theorem to get the corresponding solution $\pmod{105}$.

(B) We find that 1729 is composite because $2^{27} \equiv 654 \pmod{1729}$, $2^{54} \equiv 1065 \pmod{1729}$, $2^{108} \equiv 2^{216} \equiv 2^{432} \equiv 2^{864} \equiv 2^{1728} \equiv 1 \pmod{1729}$, and the last remainder here that isn't 1 is not -1.

On the other hand 1601 (which actually is prime) passes the test. But this does not prove it is prime.

*(C) At the fourth step we get $y_4 = 16865$, $z_4 = y_8 = 4619$, and find the factor $\gcd(16865 - 4619, 17741) = 157$. The other factor is $17741/157 = 113$.

*[5 pts each part](D) (i) For simplicity, define $N = 2^n + 1$. By definition, N is a pseudoprime to base 2 if and only if $2^{N-1} = 2^{2^n} \equiv 1 \pmod N$. Note that by the construction of N, we have $2^n \equiv -1 \pmod N$, and hence $2^{2n} \equiv 1 \pmod N$. The numbers $2, 4, 8, \ldots, 2^n$ are all less than $N - 1$, so none of them is congruent to $1 \pmod N$, and similarly for $-2, -4, -8, \ldots, -2^{n-1}$, since the are congruent to $N-2, N-4, \ldots$. So $2n$ is the smallest exponent e such that $2^e \equiv 1 \pmod N$. For any exponent e, put $e = 2nq + r$ with $r < 2n$. Then $2^e = (2^{2n})^q 2^r \equiv 2^r \pmod N$. It follows that $2^e \equiv 1 \pmod N$ if and only if $r = 0$, that is, if and only if $2n | e$. Applying this with $e = 2^n$ we see that N is a pseudoprime to base 2 if and only if $2n | 2^n$. But this clearly implies that n is a power of 2, and conversely, if n is a power of 2 then it holds, because 2^n is always greater than or equal to $2n$.

(ii) It's immediate that $2 + 1 = 3$, $2^2 + 1 = 5$, $2^4 + 1 = 17$, are prime, and $2^8 + 1 = 257$ is easy to check too. $2^{16} + 1 = 65537$ is not so easy to verify prime. Trial division requires checking all possible prime factors up to 251.

To see that 641 divides $2^{32} + 1$, either compute it explicitly: $2^{32} + 1 = 4294967297 = 641 \cdot 6700417$, or, better, compute $2^{32} \equiv -1 \pmod{641}$ by repeated squaring.