MATH 2112/CSCI 2112, Discrete Structures I
Winter 2007
Toby Kenney
Homework Sheet 5
Hints & Model Solutions

Sheet 4

5 *Define the repeat of a positive integer as the number obtained by writing it twice in a row (in decimal). For example, the repeat of 364 is 364364. Find a positive integer n such that the repeat of n is equal to m^2 for some integer m. [Hint: the repeat of n is always a multiple of n. You may find the following divisibility test useful: a number is divisible by 11 if and only if the sum of its odd digits minus the sum of its even digits is divisible by 11. For example, 1254 is divisible by 11 since the sum of its odd digits is 1+5=6 and the sum of its even digits is 2+4=6, so their difference is 0, which is divisible by 11. You won't find the answer by trial and error.]*

The repeat of a number n with k digits is $(10^k + 1)n$. If this is a square, then every prime factor of $10^k + 1$ must divide it, and must therefore also divide its square root. Thus, the square of every prime factor of $10^k + 1$ must divide $(10^k + 1)n$, so either its square will divide $10^k + 1$, or it must divide n. Since $n < 10^k + 1$, if $10^k + 1$ is not divisible by the square of any prime number, then $(10^k + 1)n$ cannot be a square. Therefore, we have to look for a positive integer k such that $10^k + 1$ is divisible by the square of some prime. To save time in our search, we can note that if k is even, then $10^k + 1 = 11 \times 90\ldots9091$. Therefore, if one of the numbers of the form $90\ldots9091$ is divisible by 11, then 11^2 will divide the corresponding $10^k + 1$. There is a useful test for divisibility by 11: add up the odd digits and subtract the even ones; if the answer is divisible by 11, then the original number was. Using this test, we see that if there are 5 '9's in the number, then it will be divisible by 11. Indeed, $10^{11} + 1 = 11^2 \times 826446281$, so the number 82644628100826446281 is a perfect square. However, this is not the repeat of a number, because it has a leading 0 – 826446281 has too few digits. To remedy this problem, we multiply 826446281 by a square number to increase the number of digits by 2. The square numbers which do this are 16, 25, 36, 49, 64, 81 and 100. These give us

$$1322314049613223140496 = 36363636364^2 \quad (1)$$
$$2066115702520661157025 = 45454545455^2 \quad (2)$$
$$2975206611629752066116 = 54545454546^2 \quad (3)$$
$$4049586776940495867769 = 63636363637^2 \quad (4)$$

$$
\begin{aligned}
528925619845289256198 4 &= 72727272728^2 && (5)\\
6694214876162942148761 &= 81818181819^2 && (6)\\
8264462810082644628100 &= 90909090910^2 && (7)
\end{aligned}
$$

These are the only solutions less than 10^{20}.

8 *Consider the integers whose last digit (in decimal) is 1. The product of any two such integers is another such integer. Any such integer can therefore be factored as a product of integers of this type that cannot be written as non-trivial products of other integers of this type. For example,* $7,211 = 11 \times 21 \times 31$*, and 11, 21, and 31 cannot be expressed as products of integers whose last digit is 1.*

Can every integer of this type be written in a unique way as such a product? Give a proof or a counterexample.

This factorisation is not unique – consider $4641 = 21 \times 221 = 51 \times 91$. The easy way to find this counterexample is to note that by unique prime factorisation for positive integers, the numbers must be composed from the same primes multiplied together in two different ways. For example, we could form the product of the 4 primes p_1, p_2, p_3, and p_4 as either $(p_1p_2)(p_3p_4)$ or $(p_1p_4)(p_3p_2)$. We want all the bracketed products to be congruent to 1 modulo 10. Therefore, $p_2 \equiv p_2(p_1p_4) = (p_2p_1)p_4 \equiv p_4 \pmod{10}$, and similarly $p_1 \equiv p_3 \pmod{10}$. This will work if $p_1 \equiv p_3 \equiv 3 \pmod{10}$ and $p_2 \equiv p_4 \equiv 7 \pmod{10}$; the smallest collection of primes of this form is 3,7,13,17. Alternatively, we could have $p_1 \equiv p_2 \equiv p_3 \equiv p_4 \equiv 9 \pmod{10}$, for example $19 \times 29 \times 59 \times 79 = 551 \times 4661 = 1121 \times 2581 = 1501 \times 1711$.

Sheet 5

1 *Use Euclid's algorithm to find the greatest common divisor of the following pairs of numbers. Write down all the steps involved.*

(a) 123,456 and 654,321

$$
\begin{aligned}
654321 &= 5 \times 123456 + 37041\\
123456 &= 3 \times 37041 + 12333\\
37041 &= 3 \times 12333 + 42\\
12333 &= 293 \times 42 + 27\\
42 &= 1 \times 27 + 15
\end{aligned}
$$

$$
\begin{aligned}
27 &= 1 \times 15 + 12 \\
15 &= 1 \times 12 + 3 \\
12 &= 4 \times 3
\end{aligned}
$$

So the greatest common divisor of 123,456 and 654,321 is 3.

(b) 1,111,111 and 12,121,212

$$
\begin{aligned}
12121212 &= 10 \times 1111111 + 1010102 \\
1111111 &= 1 \times 1010102 + 101009 \\
1010102 &= 10 \times 101009 + 12 \\
101009 &= 8417 \times 12 + 5 \\
12 &= 2 \times 5 + 2 \\
5 &= 2 \times 2 + 1 \\
2 &= 2 \times 1
\end{aligned}
$$

So the greatest common divisor of 1,111,111 and 12,121,212 is 1.

2 *Find integers* a *and* b *such that* $13579a + 2468b = 1$.

$$
\begin{aligned}
13579 &= 5 \times 2468 + 1239 \\
2468 &= 1 \times 1239 + 1229 \\
1239 &= 1229 + 10 \\
1229 &= 122 \times 10 + 9 \\
10 &= 1 \times 9 + 1
\end{aligned}
$$

So working backwards:

$$
\begin{aligned}
&1 = 10 - 9 = 10 - (1229 - 122 \times 10) = 123 \times 10 - 1229 \\
&= 123 \times (1239 - 1229) - 1229 = 123 \times 1239 - 124 \times 1229 \\
&= 123 \times 1239 - 124 \times (2468 - 1239) = 247 \times 1239 - 124 \times 2468 \\
&= 247 \times (13579 - 5 \times 2468) - 124 \times 2468 = 247 \times 13579 - 1359 \times 2468
\end{aligned}
$$

So $a = 247$, $b = -1359$ works.

3 *(a) Show that any number congruent to 3 modulo 4 is divisible by a prime number congruent to 3 modulo 4.[You may assume that the product of any collection of integers that are all congruent to 1 modulo 4 is also congruent to 1 modulo 4.]*

Proof. Suppose for contradiction that the result is not true. Let n be congruent to 3 modulo 4, but not divisible by any prime number congruent to 3 modulo 4. n is odd, so it is not divisible by 2. Therefore, all its prime factors are odd, so they must be congruent to 1 modulo 4. Their product is therefore also congruent to 1 modulo 4. This contradicts the fact that n was congruent to 3 modulo 4. Therefore, by contradiction, n must have a prime factor congruent to 3 modulo 4. □

(b) Prove that there are infinitely many prime numbers congruent to 3 modulo 4.

Hint: This is similar to the proof that there are infinitely many primes. We start by supposing that there are only finitely many prime numbers congruent to 3 modulo 4, and let them be $p_1, p_2, \ldots, p_k$. Now we take their product: $N = p_1 p_2 \cdots p_k$. Now divide into two cases: $N \equiv 1 \pmod 4$ and $N \equiv 3 \pmod 4$. In either case, we can add something to N to get a number congruent to 3 modulo 4 that isn't divisible by any of the primes that are congruent to 3 modulo 4. This will contradict (a).

4 *Are the following numbers rational or irrational? Give proofs:*
(a) $\sqrt{6}$

This is irrational.

Proof. Suppose $\sqrt{6}$ is rational. Let $p, q \in \mathbb{Z}$ such that $\frac{p}{q} = \sqrt{6}$, with $q \neq 0$. Now let $p' = \frac{p}{(p,q)}$ and $q' = \frac{q}{(p,q)}$, so that $(p', q') = 1$ and $\frac{p'}{q'} = \sqrt{6}$. Thus $p'^2 = 6q'^2$, so p'^2 is even. Therefore, p' is even. Thus $p' = 2k$ for some integer k. Therefore, $4k^2 = (2k)^2 = 6q'^2$, so $2k^2 = 3q'^2$. Therefore, q'^2 is even, so q' is even, and thus p' and q' have common factor 2. This contradicts $(p', q') = 1$, so our initial assumption that $\sqrt{6}$ is rational must be false. Therefore, $\sqrt{6}$ is irrational. □

(b) $\sqrt{2} + \sqrt{3}$ *[Hint: What is* $\left(\sqrt{2} + \sqrt{3}\right)^2$*?]*

This is irrational:

Proof. Suppose that $\sqrt{2}+\sqrt{3}$ is rational. Then $(\sqrt{2}+\sqrt{3})^2 = 2+3+2\sqrt{2}\sqrt{3} = 5+\sqrt{6}$ must also be rational. Now $5+\sqrt{6}-5 = \sqrt{6}$ is the difference of two rational numbers, and therefore rational, but it is not by (a), so by contradiction, $\sqrt{2}+\sqrt{3}$ must be irrational. □

5 *Show that the difference between a rational number and an irrational number is irrational.*

Proof. Let a be a rational number and let b be an irrational numbers. Let $c = a-b$. We want to show that c is irrational. Suppose that c is rational. Then $a-c$ is the difference between two rational numbers, and therefore, rational. However, $a-c = b$ which is irrational. This is a contradiction, so our assumption that c is rational must be impossible. Therefore, c must be irrational. □

6 *Observe that* $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\times\sqrt{2})} = \sqrt{2}^2 = 2$. *Prove that there are two irrational numbers* α *and* β *such that* α^β *is rational.*

Hint: This is a division into cases proof: Either $\sqrt{2}^{\sqrt{2}}$ is rational or it is irrational. From either of these cases, we can find α and β. This is an example of a non-constructive proof of an existential result.

7 *(Bonus Question) Prove that if a positive integer* n *is not a square, then* $\sqrt{n}$ *is irrational.*

Proof. Let the unique prime factorisation of n be $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$. Now if e_1, e_2, …, e_k are all even, then n would be a square. (If $e_i = 2f_i$ for $i = 1,\dots,k$, then n is the square of $p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}$.) Thus, at least one of $e_1, e_2, \dots, e_k$ must be odd. Let e_i be odd. Now suppose $\sqrt{n}$ is rational. Let $\sqrt{n} = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ with $q \neq 0$. Let $p' = \frac{p}{(p,q)}$ and $q' = \frac{q}{(p,q)}$. Then $\frac{p'^2}{q'^2} = n$, so $p'^2 = nq'^2$, so $p_i | p'^2$. Therefore by unique prime factorisation, $p_i|p'$ (see Sheet 4 Question 3). Therefore, since $(p', q') = 1$, p_i does not divide q'. Now $p_i^{e_i}|p'^2$, so we must have $p_i^{\frac{e_i+1}{2}}|p'$, since if the highest power of p_i dividing p' were less than $p_i^{\frac{e_i+1}{2}}$ then it would be at most $p_i^{\frac{e_i-1}{2}}$, so the highest power of p_i dividing p'^2 would be at most $p_i^{e_i-1}$, and we know that $p_i^{e_i}|p'^2$. Therefore, $p_i^{\frac{e_i+1}{2}}|p'$, and so $p_i^{e_i+1}|p'^2$. Let $p'^2 = p_i^{e_i+1}k$, then we have $p_ik = q'^2$, so $p_i|q'^2$, and thus, $p_i|q'$ This contradicts the fact that $(p', q') = 1$, so our assumption that $\sqrt{n}$ was rational must be false. Therefore, if n is not a square, then $\sqrt{n}$ is irrational. □

8 *Find* $0 \leqslant n < 2310$ *satisfying:*

$$n \equiv 7 \pmod{11} \quad (8)$$
$$n \equiv 10 \pmod{14} \quad (9)$$
$$n \equiv 11 \pmod{15} \quad (10)$$

The easy way to do this is to notice that $n = -4$ satisfies these congruences, so the unique solution with $0 \leqslant n < 2310$ (11,14, and 15 are pairwise coprime) must be congruent to -4 modulo 2310, so it must be $2310 - 4 = 2306$.

A more generally applicable way is the way used in the proof of the Chinese Remainder Theorem:

Observe that $14 \equiv 3 \pmod{11}$ and $3 \times 4 \equiv 1 \pmod{11}$, so $10 - 3 \times (4 \times 14) \equiv 10 - 3 \equiv 7 \pmod{11}$, so $n \equiv -4 \pmod{11 \times 14}$ is the unique solution to the first two congruences. Now $-4 \equiv 150 \pmod{154}$, so we need to solve the congruences

$$n \equiv 150 \pmod{154} \quad (11)$$
$$n \equiv 11 \pmod{15} \quad (12)$$

Now $154 \equiv 4 \pmod{15}$, and $4 \times 4 \equiv 1 \pmod{15}$, so $150 + 11 \times (4 \times 154) \equiv 11 \pmod{15}$, Also, $11 \times 4 = 44 \equiv 14 \pmod{15}$, so $n \equiv 150 + 14 \times 154 = 2306 \pmod{2310}$ is the unique solution.