(b) The right-to-left implication is easy: if m is an n^{th} power, then clearly $m^{1/n}$ is rational.

Now for the left-to-right implication. Suppose $m^{1/n}$ is rational; so $m^{1/n} = \frac{x}{y}$, where x,y are integers. Then $x^n = my^n$. Let p be a prime, and let p^a, p^b, p^c be the largest powers of p which divide x,y,m, respectively. Then the power of p dividing x^n is p^{an}, while the power of p dividing my^n is p^{c+bn}. By the Fundamental Theorem 11.1, we must have $an = c+bn$, and hence $c = n(a-b)$ is divisible by n.

We have shown that the power to which each prime divides m is a multiple of n; in other words, the prime factorisation of m is

$$m = p_1^{na_1} \dots p_k^{na_k}$$

for some integers a_i. Hence $m = (p_1^{a_1} \dots p_k^{a_k})^n$, and so m is an n^{th} power, as required.

7. (a) The hcf is $2 \cdot 5^2$ and the lcm is $2^2 \cdot 3 \cdot 5^3$. So the pairs (m,n) are $(2 \cdot 5^2, 2^2 \cdot 3 \cdot 5^3)$, $(2 \cdot 3 \cdot 5^2, 2^2 \cdot 5^3)$, $(2 \cdot 5^3, 2^2 \cdot 3 \cdot 5^2)$, $(2 \cdot 3 \cdot 5^3, 2^2 \cdot 5^2)$.

(b) $hcf(m,n)$ divides m, which divides $lcm(m,n)$; hence $hcf(m,n)$ divides $lcm(m,n)$. They are equal when both equal m, and similarly both equal n, i.e., when $m = n$.

(c) As in Proposition 11.2, let $m = p_1^{r_1} \cdots p_k^{r_k}$, $n = p_1^{s_1} \cdots p_k^{s_k}$. Define x to be the product of all the $p_i^{r_i}$ for which $r_i \geq s_i$, and y to be the product of all the $p_j^{s_j}$ for which $r_j < s_j$.

9. We must show the equation $x^6 - y^5 = 16$ has no solutions $x,y \in \mathbb{Z}$.

Suppose $x,y \in \mathbb{Z}$ are solutions. First suppose x is even. Then y must be even. Hence the LHS of the equation is divisible by 2^5, so it cannot equal 16.

So x must be odd. The equation is $y^5 = x^6 - 16 = (x^3-4)(x^3+4)$. The hcf of the two factors x^3-4 and x^3+4 divides their difference, 8. As both are odd numbers (since x is odd), we deduce that $\text{hcf}(x^3-4, x^3+4) = 1$. So x^3-4, x^3+4 are coprime numbers with product equal to the fifth power y^5. By Proposition 11.4(b), this implies that both x^3-4 and x^3+4 are fifth powers. But two fifth powers clearly cannot differ by 8 (the fifth powers are $\dots, -32, -1, 0, 1, 32, \dots$). Hence there are no solutions.

Chapter 12

1. One of the three numbers $p, p+2, p+4$ must be divisible by 3. Since they are all supposed to be prime, one of them must therefore be equal to 3, so the only possibility is $p = 3$.

3. For $n = 5,6,7,8,9,10$ we have $\phi(n) = 4,2,6,4,6,4$, respectively.

If p is prime then all the numbers $1,2,\dots,p-1$ are coprime to p, and hence $\phi(p) = p-1$.

For $r \geq 1$, the numbers between 1 and p^r which are *not* coprime to p^r are those which are divisible by p, namely, the numbers kp with $1 \leq k \leq p^{r-1}$. There are p^{r-1} such numbers, and hence $\phi(p^r) = p^r - p^{r-1}$.

5. $x = 40$ will do nicely.

Chapter 13

1. (a) $7^2 \equiv 5 \bmod 11$, so $7^4 \equiv 5^2 \equiv 3 \bmod 11$ and so $7^5 \equiv 3.7 \equiv -1 \bmod 11$. Therefore $7^{135} \equiv (-1)^{27} \equiv -1 \bmod 11$, so $7^{137} \equiv -7^2 \equiv 6 \bmod 11$. So $r = 6$.

(b) Use the method of successive squares from Example 13.3. Calculate that $2^{16} \equiv 391 \bmod 645$ and $2^{64} \equiv 256 \bmod 645$. Hence $2^{81} = 2^{1+16+64} \equiv 2 \cdot 391 \cdot 256 \equiv 242 \bmod 645$.

(c) We need to consider 3^{124} modulo 100. Observe $3^5 \equiv 43 \bmod 100$, so $3^{10} \equiv 49 \bmod 100$ and then $3^{20} \equiv 1 \bmod 100$. Hence $3^{120} \equiv 1 \bmod 100$, and so $3^{124} \equiv 3^4 \equiv 81 \bmod 100$. Therefore the last two digits of 3^{124} are 81.

(d) The multiple $21n$ will have last 3 digits 241 if $21n \equiv 241 \bmod 1000$. Since $\text{hcf}(21,1000) = 1$, such an n exists, by Proposition 13.6.

3. (a) There is a solution by Proposition 13.6, as $\text{hcf}(99,30) = 3$ divides 18. To find a solution, observe first that $3 = 10 \cdot 30 - 3 \cdot 99$. Multiplying through by 6, we get $18 = 60 \cdot 30 - 18 \cdot 99$, hence $-18 \cdot 99 \equiv 18 \bmod 30$. So $x = -18$ is a solution.

(b) There is no solution by Proposition 13.6, as $\text{hcf}(91,143) = 13$ does not divide 84.

(c) The squares $0^2, 1^2, 2^2, 3^2, 4^2$ are congruent to $0,1,4,4,1$ modulo 5, respectively. Since any integer x is congruent to one of $0,1,2,3,4$ modulo 5, it follows that x^2 is congruent to 0, 1 or 4. Hence the equation $x^2 \equiv 2 \bmod 5$ has no solution.

(d) Putting $x = 0,1,2,3,4$ gives x^2+x+1 congruent to $1,3,2,3,1$ modulo 5, respectively. Hence the the equation $x^2+x+1 \equiv 0 \bmod 5$ has no solution.

(e) $x = 2$ is a solution.

5. (a) Since $7 | 1001$, we have $1000 \equiv -1 \bmod 7$, so $1000^2 \equiv 1 \bmod 7$, $1000^3 \equiv -1 \bmod 7$, etc. So the rule is to split the digits of a number n into chunks of size 3 and then alternately add and subtract — then the answer is divisible by 7 if and only if n is. The number 6005004003002001 is congruent modulo 7 to $1-2+3-4+5-6 = -3$, so the remainder is 4.

(b) Same rule as for 7. The number is again congruent to -3 modulo 13, so the remainder is 10.

(c) Since $1000 \equiv 1 \bmod 37$, $1000^2 \equiv 1 \bmod 37$, etc., the rule is to split the digits of a number n into chunks of size 3 and then add — the answer is divisible by 37 if and only if n is. The given number is congruent modulo 37 to $1+2+3+4+5+6=21$.

7. Consider a square n^2. As in Exercise 2(c), $n^2 \equiv 0,1$ or $4 \bmod 5$. Similarly, we see that $n^2 \equiv 0,1$ or $4 \bmod 8$.

We first show n is divisible by 5. We know that the squares $2n+1$ and $3n+1$ are congruent to 0,1 or -1 modulo 5. Say $2n+1 \equiv a \bmod 5, 3n+1 \equiv b \bmod 5$, with $a,b \in \{0,1,-1\}$. If $a \neq b$, then adding gives $5n+2 \equiv 2 \equiv a+b \bmod 5$; but this cannot hold when $a \neq b$ and $a,b \in \{0,1,-1\}$. So $a=b$; then subtracting gives $n \equiv b-a \bmod 5$; hence as $a=b$, we get $n \equiv 0 \bmod 5$, i.e., n is divisible by 5.

Now we show n is divisible by 8 in exactly the same way. Hence n is divisible by 40.

The first value of n that works is 40, since then $2n+1=81$ and $3n+1=121$ are squares.

Another value of n that works is 3960, since then $2n+1=7921=89^2$ and $3n+1=11881=109^2$.

9. The equation $ax=b$ has a solution for $x \in \mathbb{Z}_p$ if and only if the congruence equation $ax \equiv b \bmod p$ has a solution. Since $a \neq 0$ in $\mathbb{Z}_p$, a and p are coprime, so there is a solution by Proposition 13.6.

11. The number of days in 1000 years is $1000 \times 365 + 250$ (the 250 for the leap years). Since $365 \equiv 1 \bmod 7$, this is congruent to 1250 modulo 7, which is congruent to 4 modulo 7. Hence May 6, 3005 will in fact be a Tuesday.

Chapter 14

1. (a) By Fermat's Little Theorem, $3^{10} \equiv 1 \bmod 11$, so $3^{301} = 3^{300} \cdot 3 \equiv 3 \bmod 11$. In other words, $3^{301} \pmod{11} = 3$. Likewise, we have $5^{110} \pmod{13} = 12$ and $7^{1388} \pmod{127} = 49$.

(b) By Fermat's Little Theorem, $n^7 \equiv n \bmod 7$. Also $n^3 \equiv n \bmod 3$, and hence $n^7 = n^3 \cdot n^3 \cdot n \equiv n^3 \equiv n \bmod 3$. Clearly also $n^7 \equiv n \bmod 2$. Hence $n^7 - n$ is divisible by 2, 3 and 7, hence by 42, i.e., $n^7 \equiv n \bmod 42$.

3. Let a be coprime to 561. Then by Fermat, $a^{16} \equiv 1 \bmod 17$, $a^{10} \equiv 1 \bmod 11$

and $a^2 \equiv 1 \bmod 3$. So

$$a^{560} \equiv (a^{16})^{35} \equiv 1 \bmod 17,$$
$$a^{560} \equiv (a^{10})^{56} \equiv 1 \bmod 11,$$
$$a^{560} \equiv (a^2)^{280} \equiv 1 \bmod 3,$$

and hence $a^{560}-1$ is divisible by 3, 11 and 17, hence by $3 \cdot 11 \cdot 17 = 561$. So $a^{560} \equiv 1 \bmod 561$.

5. By Fermat, $p^{q-1} \equiv 1 \bmod q$. Since $q^{p-1} \equiv 0 \bmod q$, this implies that $p^{q-1} + q^{p-1} \equiv 1 \bmod q$. Similarly, $p^{q-1} + q^{p-1} \equiv 1 \bmod p$. Hence $p^{q-1} + q^{p-1} - 1$ is divisible by both p and q, hence by pq, and so $p^{q-1} + q^{p-1} \equiv 1 \bmod pq$.

7. (a) Use the recipe provided by Proposition 14.2. Since $3 \cdot 19 \equiv 1 \bmod 28$, the solution is $x \equiv 2^{19} \bmod 29$. Using successive squares, this is $x \equiv 26 \bmod 29$.

(b) Notice cleverly that $143 = 11 \cdot 13$, so we use the recipe of Proposition 14.3. Here $(p-1)(q-1) = 120$, and $7 \cdot 103 \equiv 1 \bmod 120$. So the solution is $x \equiv 12^{103} \bmod 143$. Since $12^2 \equiv 1 \bmod 143$, the solution is $x \equiv 12 \bmod 143$.

(c) Again use 14.3. Since $11 \cdot 11 \equiv 1 \bmod 120$, the solution is $2^{11} \pmod{143}$, which is $46 \pmod{143}$.

9. Use successive squares to calculate that $2^{1386} \equiv 1 \bmod 1387$, but $2^{693} \equiv 512 \bmod 1387$. So Miller's test shows that 1387 is not prime.

Chapter 15

1. We have $p+q = pq-(p-1)(q-1)+1 = 18779-18480+1 = 300$. Hence p,q are the roots of $x^2-300x+18779=0$. Using the formula for the roots of a quadratic, these are $\frac{1}{2}(300 \pm \sqrt{300^2-4 \cdot 18779})$, i.e., 211 and 89.

3. To crack this code, observe that $1081 = 23 \cdot 47$. Taking $p=23, q=47$, we have $(p-1)(q-1) = 1012$. Since $e=25$ and $25 \cdot 81 \equiv 1 \bmod 1012$, the decoding power $d=81$. So the decoded message starts with $23^{81} \pmod{1081} = 161$, then $930^{81} \pmod{1081} = 925$, then $228^{81} \pmod{1081} = 30$, and finally $632^{81} \pmod{1081} = 815$. So the decoded message is 161925030815, which with the usual letter substitutions (A for 01, etc.), is PSYCHO. Good choice, Ivor!