Solutions to Exercises 1 to 47

1 a) You get:

(Note the short-cut : 54−51 !)

$a = 129$	$1728 = b$
$-26a + 2b = 102$	$1677 = 13a$
$27a - 2b = 27$	$51 = -13a + b$
27	$54 = 54a - 4b$
0	$3 = 67a - 5b$

b) If $ax + by = 1$ and $ax' + by' = 1$ then (subtract) $a(x - x') = -b(y - y')$

Since a, b are coprime, then a divides $y - y'$ and so $x - x'$ is a multiple of b.

c) If $\text{hcf}(a,b) = d$ and $ax + by = d$ then divide through by d and use part b) to deduce that x is determined up to a multiple of $\frac{b}{d}$.

2 If we have $pr + qs = 1$ and take $x = prb + qsa$ then working mod p gives $qs = 1$ and $x = qsa = a$ while working mod q gives $pr = 1$ and $x = prb = b$. Thus x satisfies both congruences.

If x_1 and x_2 are both solutions then subtract to get $x_1 - x_2 = 0 \mod p$ and $\mod q$.

Since p and q are coprime it follows that pq divides $x_1 - x_2$. i.e. the solution is unique up to multiples of pq.

By the Euclidean algorithm $1 = \overset{p}{13}(\overset{r}{-3}) + \overset{q}{8}(\overset{s}{5})$ and so the solution is $13(-3)7 + 8(5)5$ $= -273 + 20 = -73$ and the solution is unique mod 104. So we may take $+31$ as the answer.

3 a) Euclid's proof does not guarantee that $p_1 p_2 \cdots p_n + 1$ is prime — just that this is not divisible by $p_1, \ldots, p_n$. The smallest counterexample is $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031$ which is 59×509.

b) The same argument applies to $p_1 p_2 \cdots p_n - 1$. This time $2 \times 3 \times 5 \times 7 - 1 = 209$ $= 11 \times 19$.

4 In fact <u>any</u> number of the form $4n-1$ cannot have all its factors of the form $4n+1$ since the product of numbers which are $1 \pmod 4$ is also $1 \pmod 4$.

So follow Euclid and suppose that $q_1, q_2, \ldots, q_n$ were the only primes of the form $4k-1$. Then $4q_1q_2 \cdots q_n - 1$ would have to have a factor of this form which is impossible since division by q_i leaves a remainder.

Unfortunately the same argument will not work for primes of the form $4k+1$ because a product of the form $4q_1q_2 \cdots q_n + 1$ with the q_i all the $4k+1$ primes might have factors of the form $4k-1$ (e.g. 21 is of the form $4k+1$ but is divisible by 3 and 7.) In fact there <u>are</u> infinitely many primes of the form $4k+1$, but the proof is harder.

5 The first ten "Hilbert primes" are:

5, 9, 13, 17, 21, 29, 33, 37, 41, 49.

e.g. Although $21 = 3 \times 7$ the numbers $3, 7 \notin H$.

Then $693 = 3 \times 3 \times 7 \times 11$ and can be written as a product of Hilbert primes either as $693 = 21 \times 33$ or $693 = 9 \times 77$.

6 $(x,y) \mapsto 5x+3y$ maps $(2,1) \in \mathbb{Z}_3 \times \mathbb{Z}_5$ to $1 \in \mathbb{Z}_{15}$ and so can be extended to a map of the additive groups. ($(2a,a) \mapsto a \in \mathbb{Z}_{15}$). However, it does not map the multiplicative identity $(1,1)$ of $\mathbb{Z}_3 \times \mathbb{Z}_5$ to $1 \in \mathbb{Z}_{15}$ and so is not a ring homomorphism. The map $(x,y) \mapsto 10x+6y$ <u>does</u> map the multiplicative identities properly and does give a ring homomorphism.

More generally, if m,n are coprime with $1 = ma+nb$ then the map $(x,y) \mapsto nbx+may$ maps $(1,0)$ to $nb \in \mathbb{Z}_{mn}$ (an element of order a) and $(0,1)$ to ma (an element of order b) and maps $(1,1)$ to $1 \in \mathbb{Z}_{mn}$ as required.

7. $2^5 = 32 = -1 \pmod{11}$ and $1 \pmod{31}$. Thus $2^{10} = 1 \pmod{11}$ and $1 \pmod{31}$ and so $1 \pmod{341}$. Thus $2^{340} = 1 \pmod{341}$ $[341 = 11 \times 31]$.

Note that $91 = 7 \times 13$. $3^6 = 1 \bmod 7$ by Fermat's Little Theorem (FLT) and $3^3 = 27 = 1 \pmod{13}$

So $3^6 \equiv 1$ (mod 7 and mod 13) and hence $\equiv 1 \pmod{91}$ //
So $3^{90} \equiv 1 \pmod{91}$

If $3^{340} \equiv 1 \pmod{341}$ then $3^{340} \equiv 1 \pmod{31} \Rightarrow$ (since $3^{30} \equiv 1 \pmod{31}$ by FLT). $3^{10} \equiv 1 \pmod{31}$ which is not true $[3^5 \equiv 5 \pmod{31} \Rightarrow 3^{10} \equiv 25 \bmod 31]$

Hence 341 is not a pseudo-prime wrt 3 //

If $2^{90} \equiv 1 \pmod{91}$ then $2^{90} \equiv 1 \pmod{13} \Rightarrow$ (since $2^{12} \equiv 1 \pmod{13}$ by FLT) $2^6 \equiv 1 \pmod{13}$ which is not true. Thus 91 is not a pseudoprime wrt 3 //

? Strong pseudo primes. As above, $2^{10} \equiv 1 \pmod{341}$

Thus $2^{170} \equiv 1 \pmod{341}$ but $2^{85} \equiv 2^5 = 32 \pmod{341}$ and so 341 is not a strong pseudo-prime wrt 2. //

Similarly since $3^6 \equiv 1 \pmod{91}$ we calculate $3^{45} \equiv 3^3 \pmod{91}$ and this is not ± 1 so 91 is not a strong pseudo-prime wrt 3.

By FLT if a is coprime to $1105 = 5 \times 13 \times 17$ we have $a^4 \equiv 1 \pmod 5$; $a^{12} \equiv 1 \pmod{13}$ and $a^{16} \equiv 1 \pmod{17}$ and since $1104 = 16 \times 3 \times 23$, it follows that $a^{1104} \equiv 1$ (mod each of 5, 13, 17) and hence mod 1105.

To show that 1105 is not a <u>strong</u> pseudoprime wrt 2, we calculate 2^{552} and 2^{276} mod 1105. As before calculate separately mod 5, 13, 17. Since 276 is divisible by 4 and 12 we have $2^{276} = 2^{552} = 1 \bmod 5$ and mod 13. Also $2^4 = -1 \bmod 17$ and so $2^8 = 1 \bmod 17 \Rightarrow 2^{276} = 2^4 = -1 \bmod 17$, while $2^{552} = +1 \bmod 17$. Hence $2^{552} = 1 \bmod 1105$ but $2^{276} \neq \pm 1 \bmod 1105$ and so 1105 is <u>not</u> a strong pseudoprime

8 By FLT $a^2 = 1 \pmod 3$, $a^{10} = 1 \pmod{11}$, $a^{16} = 1 \pmod{17}$
$\Rightarrow a^{560} = 1$ (mod all three) $\Rightarrow a^{560} = 1 \pmod{3 \times 11 \times 17}$ (provided a is coprime to 3, 11, 17). //

Similarly, $a^6 = 1 \pmod 7$, $a^{12} = 1 \pmod{13}$, $a^{18} = 1 \pmod{19}$ and since 1728 is divisible by 6, 12, 18 we get $a^{1728} = 1 \pmod{1729}$ if a is coprime to 7, 13, 19 //

This is the case $t = 1$ of the following.

Let $N = (6t+1)(12t+1)(18t+1)$ and observe (work mod 12 and mod 18) that $N-1$ is divisible by 12 and 18. Then, as above, $a^{N-1} = 1 \pmod N$.

The first $t > 1$ giving primes is $t = 6 \Rightarrow$
$N = 37 \times 73 \times 109 = 294409$ is Carmichael.

Maple gives 842 values of $t < 100000$ leading to primes.

9. (i) You need (at least) 4 multiplications to get to a^{16} and so 5 to get a^{17} : 2, 4, 8, 16, 17.

(ii) The "obvious" way : 2, 4, 8, 16, 24, 26, 27 needs 7 multiplications. You can manage with only 6 : 2, 3, 6, 12, 24, 27

(iii) You can use 7 : 2, 4, 8, 16, 32, 36, 37 or : 2, 4, 8, 12, 24, 36, 37 or ...

(iv) Standard way : 2, 4, 8, 16, 32, 40, 44, 46, 47

Better : 2, 3, 4, 8, 11, 22, 44, 47

(v) Standard way : 2, 4, 8, 16, 32, 48, 56, 57 and I can't find anything shorter.

10. If p is not prime then for all the primes q dividing p we have $(p-1)! = 0 \bmod q$. Hence $(p-1)! = 0 \pmod p$

11 a) p, q are distinct and so work $\pmod p$: $N = p^{q-1} + q^{p-1} = q^{p-1} = 0$ by FLT. Similarly $N = 0 \pmod q$ and so is $0 \pmod{pq}$

b) a, b are coprime mod p and so $a^{p-1} = 1$ and $b^{p-1} = 1 \bmod p \Rightarrow a^{p-1} - b^{p-1} = 0 \bmod p$.

If $p = 4$ (say) then $2^3 - 1^3 \neq 0 \bmod 4$

12. Any prime factor of 2^m-1 is of the form $2mk+1$ so for $2^{23}-1$ the first candidate is 47 which is a factor. The other factor 178481 is in fact prime and is $46\times 3880+1$.

For $2^{29}-1$ possibilities are 59, $\cancel{117}$, $\cancel{175}$, 233 which is a factor. In fact $2^{29}-1 = 233\times 1103\times 2089$ $=(58\times4+1)(58\times19+1)(58\times36+1)$

13. A triangular number is one of the form $\frac{1}{2}(k-1)k$

An even perfect number is of the form $\frac{1}{2}2^m(2^m-1)$

so take $k=2^m$.

If $p=2^m-1$ is prime, the divisors of $n=2^{m-1}p$ are $1, 2, \ldots, 2^{m-1}, p, 2p, \ldots, 2^{m-1}p$ (including n itself).

So use the sum of a GP formula to get: the sum of the reciprocals is $\left(1+\frac{1}{p}\right)\left(1+\frac{1}{2}+\cdots+\frac{1}{2^{m-1}}\right)=\frac{p+1}{p}\left(\frac{1-\frac{1}{2^m}}{1-\frac{1}{2}}\right)$ $=2$.

14. We can write 24 as $3\times2\times2\times2$ or $2\times3\times2\times2$ or $2\times2\times3\times2$ or $2\times2\times2\times3$. In other words the 3 can go into one of 4 places among the 2s.

For the $72 = 2^3 \times 3^2$ case or for the general case $2^\alpha 3^\beta$ you can argue as follows.
Lay out $\alpha+\beta$ counters which have a 2 on the top and a 3 underneath. To get a factorisation you need to turn over β of the counters. You can choose these in $\binom{\alpha+\beta}{\beta} = \frac{(\alpha+\beta)!}{\alpha!\beta!}$ different ways. So the answer for 72 is $\frac{5!}{2!3!} = 10$.

You can try and see that for the general problem $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ the number of factorisations is the "multinomial coeff" $\frac{(\alpha_1+\dots+\alpha_k)!}{\alpha_1!\alpha_2!\dots\alpha_k!}$

e.g. $2^3 3^2 5^2 = 1800$ has $\frac{7!}{3!2!2!} = 210$ "different" factorisations.

15 Since the sum is even, both numbers are either even or odd. If both are even then $ab(a+b)$ is divisible by 8. If both are odd then $a-b$ differs from $a+b$ by $2\times$odd number and so both $a+b$ and $a-b$ are even and one is divisible by 4. Hence $(a+b)(a-b)$ is divisible by 8.
To show that $ab(a^2-b^2)$ is divisible by 3:

either one of $a, b = 0 \bmod 3$, or they are equal (mod 3) or one is $1 \pmod 3$ and the other is $2 \pmod 3$. In each case the product is $0 \pmod 3$. The result follows. [Note: we don't need the fact that a, b are coprime!]

16. $\binom{p}{k}$ is an integer — for combinatorial reasons! Since $\binom{p}{k} = \frac{p!}{(p-k)!k!}$ there is nothing in the denominator to cancel the p in the numerator and so the integer is divisible by p.

To prove FLT: take p prime and we'll prove $a^p = a \pmod p$ by induction on a. It's OK at $a=1$. Then $(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \dots + \binom{p}{p-1}a + 1 = a^p + 1 \pmod p$ by the last result. Hence the induction follows.

$\binom{p-1}{k} = \frac{(p-1)(p-2)\dots(p-k)}{1 \cdot 2 \cdot \dots \cdot k}$ and since $p-1 = -1$, $p-2 = -2, \dots$ the result follows.

One can see this instead by observing that in Pascal's Δ mod p, the pth line is $1\,0\,0 \dots 0\,1$ and so the line above must alternate: $1\ {-1}\ 1\ {-1} \dots 1$.

17 If $q = \left[\frac{n}{p}\right]$ (integer part!) is the largest multiple of $p \leq n$ the product $n!$ will contain a copy of $p, 2p, \ldots, qp$. If in addition $p^2 \leq n$ there will be an "extra" copy of p for each multiple of p^2 in the product $1.2.\ldots.n$ and so on.

There will be a zero at the end of $n!$ for each power of 5 dividing $n!$ (since there are plenty of 2s to go with them).

Thus $100!$ has $\left[\frac{100}{5}\right] + \left[\frac{100}{25}\right] = 24$ zeros.

$1000!$ has $\left[\frac{1000}{5}\right] + \left[\frac{1000}{25}\right] + \left[\frac{1000}{125}\right] + \left[\frac{1000}{625}\right] =$

$200 + 40 + 8 + 1 = 249$ zeros.

18 We'll prove Bertrand's conjecture ($\varepsilon = 1$) using Chebyshev's version of the PNT ($\pm 10\%$ say).

i.e. $0.9 \frac{n}{\log n} < \pi(n) < 1.1 \frac{n}{\log n}$. Then

$\pi(2n) > 0.9 \frac{2n}{\log 2n} \underset{*}{>} \frac{0.9 \times 2n}{1.2 \log n}$ (*provided

$\log 2n < 1.2 \log n$ or $0.2 \log n > \log 2$ or $n > 32$)

and $\pi(n) < 1.1 \frac{n}{\log n} \Rightarrow \pi(2n) - \pi(n) >$

$\frac{n}{\log n} \left\{ \frac{0.9 \times 2}{1.2} - 1.1 \right\} = 0.4 \frac{n}{\log n} > 1$ if $n \geqslant 4$.

19. Since p is prime, multiplying through by $(p-1)!$ will not alter the divisibility of the numerator — but it will give an integer. So we calculate

$(p-1)!\left\{1 + \frac{1}{2} + \dots + \frac{1}{p-1}\right\} (\text{mod } p) = -\left\{1^{-1} + 2^{-1} + \dots + (p-1)^{-1}\right\}$

since $(p-1)! = -1 \pmod p$ [Wilson's theorem — though we don't need it!] and the sum in brackets $\{\}$ is the sum of all the elements of $\mathbb{Z}_p - \{0\}$ and so they all cancel out mod p.

e.g. $1 + \frac{1}{2} + \dots + \frac{1}{19} = \frac{14274301}{4084080}$ and the numerator is $19^2 \times 39541$. Wolstenholm also proved the numerator of $1 + \frac{1}{2^2} + \dots + \frac{1}{(p-1)^2}$ is divisible by p if p is a prime > 3

20 A square of a number ending in digits ab will be (mod 100) $(10a+b)^2 = 20a+b$. So the possible endings are:

00	01	04	25	16	09	i.e. 22 possible
	21	24		36	29	out of 100.
	41	44		56	49	
	61	64		76	69	
	81	84		96	89	

If $N = 33490021 + y^2 = x^2$ we must find two numbers in the list 21 apart (mod 100).
That is 00 and 21 or 04 and 25.

So y can end in $*0$ or 02 or 52 or 48 or 98. Going through the possibilities (with a calculator!) one rejects 19 of them until one reaches $y = 150$ to get $N + 150^2 = 5789^2$
So the factors are $5789 \pm 150 = 5639$ and 5939.

21 Start with $x_1 = 2$ to get a sequence

i	1	2	3	4	5	6	7	8	9	10	11	12
x_i	2	5	26	286	<u>78</u>	220	308	243	9	82	<u>78</u>	220
$x_i - x_{i/2}$		3		281		194		-43		4		0

and in this case $N = \text{hcf}$. So start again with (say 5) to save calculation!:

i	1	2	3	4	5	6	7	8
x_i	5	26	286	78	220	308	243	9
$x_i - x_{i/2}$		21		52		22		-69

and in this case the hcf $= 23$ and we have found a factor.

You can write a Maple program like:

```
n := 1822338014407l ;
f := x -> (x*x+1) mod n :
x := 2 :   S := [x]:
for i from 2 to 6000 do
   x := f(x) ;  S := [op(S), x];
   if i mod 2 = 0 then
      m := igcd(x - S[i/2], n);
      if m>1 then print(i, m); end if;
   end if;
end do :
```

This discovers the factor 5447899 after 5332 steps (and the other factor 3345029) after 5508 steps.

22 $(2^9+2^7+1)(2^{23}-2^{21}+2^{19}-2^{17}+2^{14}-2^9-2^7+1) =$

$$\begin{aligned}
&2^{32}-2^{30}+2^{28}-2^{26}+2^{23}-2^{18}-2^{16}+2^9\\
&\quad+2^{30}-2^{28}+2^{26}-2^{24}+2^{21}-2^{16}-2^{14}+2^7\\
&\qquad\qquad+2^{23}-2^{21}+2^{19}-2^{17}+2^{14}\\
&\qquad\qquad\qquad-2^9-2^7+1\\
&= 2^{32}+2^{24}-2.2^{23}+2^{19}-2^{18}-2^{17}-2.2^{16}+1\\
&= 2^{32}+1.
\end{aligned}$$

Note that $2^9+2^7+1 = 641$ as Euler discovered.

23 UNBREAKABLE $\Rightarrow$ WOPSSBMBPMS
BANANABANAN

Decoding means shifting <u>down</u> at each letter:

LYXLERQPNAXUQURWPRJPREVNAJRZFHW
CATCATCATCATCATCATCATCATCATCATC
IXDIDXNOTXWANTXTOXGOXBUTXIXWENT

Since moving down n (mod 26) is the same as moving up $26-n$ one can decode by coding with the "complementary" key-word. For CAT this is WYF.

Note that the Vigenère cipher is subject to attack using "frequency analysis" if one knows the <u>length</u> of the key word. There are cunning methods for guessing this. So a short key word is dangerous to use. If the key word is longer than the message (this is called a "one time pad") the cipher is provably uncrackable.

24 The product of 3 (or more) distinct primes will be OK. The same proof as in lectures (with $m = \mathrm{lcm}(p-1, q-1, r-1)$) still works. Things go wrong if you take the square of a prime. Here you can code and decode in $U_{p^2} \subset \mathbb{Z}_{p^2}$, but taking powers of anything in $\mathbb{Z}_{p^2} - U_{p^2}$ (where things are multiples of p) will always give $0 \pmod{p^2}$ and so one does not get a 1-1 map).

25 $\phi(pq) = (p-1)(q-1)$. So $n - \phi(n) = pq - (p-1)(q-1) = p+q-1$. $(p+q)^2 - (p-q)^2 = 4pq = 4n$. So if one knows n <u>and</u> $\phi(n)$ one can find $p-q$ and $p+q$ and hence p and q.

If $n = 14933$ and $\phi(n) = 14688$ then $p+q = 246 \Rightarrow p-q = 28 \Rightarrow p = 137,\ q = 109$.

26 $N = 1003$, $m = \mathrm{lcm}(p-1, q-1) = \mathrm{lcm}(16, 58) = 16 \times 29 = 464$. Solve $3x = 464 + 1 \Rightarrow x = 155$ so this is the decoding power.

Coding STANDREWS using the suggested method and a block length of 3 gives (in blocks of 3)
192, 001, 140, 418, 052, 319
and this is (just) within range of a calculator to get coded groups:
720, 001, 795, 184, 188, 667

Decoding involves raising the 3 digit numbers to the power of 155 so it's no job for a calculator. Using a computer (and Maple) gives the groups:

142, 113, 020, 518, 200, 805, 151, 825

and (splitting this up into blocks of length 2) gives

NUMBERTHEORY.

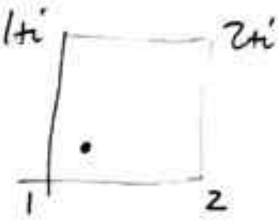
27 Attempting either of them "by hand" will convince you they "must be true"!

In fact a) is <u>false</u> but the smallest counterexample is 905.

b) is called Goldbach's conjecture and dates back to 1742. If there is a counterexample it has more than 18 digits, but no proof is yet known.

28 a) Divide in $\mathbb{C}$: $\frac{2+3i}{2+2i} = \frac{1}{2}\cdot\frac{(2+3i)(1-i)}{2}$

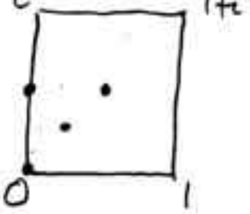
$= \frac{1}{4}(5+i)$ and so is within 1 of $1, 1+i, 2$



So quotients, remainders are: $(1, i), (1+i, 2-i), (1, -2-i)$

(each remainder smaller than 8 in norm.)

b) Choose numbers so that quotients lie as shown in the square:



(i) $(1+i, 2)$ (ii) $(1+i, 4)$
(iii) $(i, 2)$ (iv) $(0, 1)$ (There are many other solutions!)

29 a) $N(9+5i) = 106 = 2\times 53$ and $2 = 1^2+1^2$, $53 = 7^2+2^2$

So possible factors are $1\pm i$, $7\pm 2i$. Experiment to get $(1+i)(7+2i) = 5+9i \Rightarrow$ (conjugate!) $(1-i)(7-2i) = 5-9i \Rightarrow 9+5i = i(1-i)(7-2i)$ //

$14+10i = 2(7+5i)$ so work with the second factor: $N(7+5i) = 74 = 2\times 37$ so possible factors are $(1\pm i)$ and $(6\pm i)$. Experiment to get $(1+i)(6+i) = 5+7i \Rightarrow i(1-i)(6-i) = 7+5i$.
So factorisation is: $i(1-i)^2(1+i)(6-i)$.

$N(55+i) = 3026 = 2 \times 17 \times 89$ after some calculator work (need only check primes of the form $4k+1$). Possible factors are $1 \pm i$, $1 \pm 4i$, $8 \pm 5i$

Experiment $\Rightarrow (1-4i)(8+5i)(1+i) = 55+i$.

29b) Same method $\Rightarrow 5+3i = (1+i)(1+4i)$ and $7+9i = (1+i)(1+2i)(2-3i)$. So hcf $=$ $(1+i)$. It is unique up to multiplication by units so $\pm 1 \pm i$ would work equally well.

Note that $N(5+3i) = 34$ and $N(7+9i) = 110$ and the hcf of these numbers is 2 so both numbers are divisible by an irreducible of norm 2 which (up to multiplication by units) must be $1+i$.

30 a) If m, n can be written (resp) as a^2+b^2 and c^2+d^2 then $m = N(a+bi)$, $n = N(c+di)$ and taking the product $N((a+bi)(c+di)) = (a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (bc+ad)^2$.

b) $725 = 5^2 \times 29$ and so we find Gaussian integers with this as norm. $N(2 \pm i) = 5$, $N(5 \pm 2i) = 29$

Take $(2+i)(2-i)(5+2i) = 25+10i \Rightarrow 25^2+10^2$

$(2+i)^2(5+2i) = (3+4i)(5+2i) = 7+26i \Rightarrow 7^2+26^2$

$(2+i)^2(5-2i) = (3+4i)(5-2i) = 23+14i \Rightarrow 23^2+14^2$

and these are the only possibilities.

$20808 = 2^3 \times 3^2 \times 17^2$. The factor 3^2 cannot be split further. $N(1 \pm i) = 2$, $N(4 \pm i) = 17$.

Take $3(1+i)^2(1-i)(4+i)^2 = 6(1+i)(15+8i) =$

$6(7+23i) = 42 + 138i \Rightarrow 42^2 + 138^2$.

or $3(1+i)^2(1-i)(4+i)(4-i) = 6 \times 17(1+i) =$

$102 + 102i \Rightarrow 102^2 + 102^2$

c) If a number has two factors of the form $4k+1$ (and all factors of the form $4k+3$ occurring as squares) then it can be written as a sum of squares in more than one way.

The smallest number which can be written as a sum of squares in three ways is $5^2 \times 13 = 325$.

To get four ways you need at least $5^3 \times 13 = 1625$.

31. $(1 \pm i)^2 = \pm 2i \Rightarrow (1 \pm i)^4 = -4$. Note that taking 4th powers of a complex number multiplies the argument by 4 and so if $z^4 \in \mathbb{R}$, $\text{Arg}(z)$ is a multiple of $\frac{\pi}{4}$ (45°) and so z is a multiple of $1+i$.

Hence z^4 will be an integer 4th power $\times -4$.

The same reasoning shows that there are no integers whose cube roots are in $\mathbb{Z}[i]$ but not in $\mathbb{Z}$.

32. $N(2) = 4$ and $N(1 \pm \sqrt{-3}) = 4$ and there are no elements in $\mathbb{Z}[\sqrt{-3}]$ with norm 2, so these are irreducible. Hence $4 = 2 \times 2 = (1+\sqrt{-3})(1-\sqrt{-3})$ is written in two distinct ways as a product of irreducibles.

Similarly $6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$

33 $N(a+b\sqrt{d})N(A+B\sqrt{d}) = (a^2+db^2)(A^2+dB^2)$ and $N((a+b\sqrt{d})(A+B\sqrt{d})) = (aA+bBd)^2+d(aB+bA)^2$ and one may check these are the same.

In $\mathbb{Z}[\sqrt{2}]$ we can write $7 = (3+\sqrt{2})(3-\sqrt{2})$.

If 5 were reducible then its factors would have norms dividing $N(5) = 25$. and so we would need an element $a+b\sqrt{2}$ with $a^2-2b^2 = 5$. Squares mod 5 can only be $0, 1, 4$ and the only solutions mod 5 would be $a = b = 0$ mod 5. It's easy to see that can't happen.

Irreducible elements in $\mathbb{Z}[\sqrt{2}]$ are $a+0\sqrt{2}$ or $0+a\sqrt{2}$ with $a = \pm 2$ or $\pm p$ for p a prime of the form $8k\pm 3$ or elements $a+bi$ with norm a prime — which would necessarily be of the form $8k \pm 1$

34. $N(a+b\omega) = |a+b\omega|^2 = (a+b\omega)(a+b\bar{\omega})$
$= a^2+b^2+ab(\omega+\bar{\omega}) = a^2+b^2-ab.$
Since $N(uv) = N(u)N(v)$ if u is invertible we must have $N(u)$ invertible in $\mathbb{Z} \Rightarrow N(u) = 1$.

So the units lie on the unit circle $|z|=1$ and the only elements of $\mathbb{Z}[\omega]$ on this are $\pm 1, \pm\omega, \pm(1+\omega)$.

Multiplying a prime by a unit still gives a prime and since multiplying by ω represents rotation by $\pi/3$ the set of primes has 6-fold rotational symmetry. It also has reflective symmetry in the real and imaginary axes.

If a <u>real</u> prime n is not a prime in $\mathbb{Z}[\omega]$ it can be written as a product $(a+b\omega)(a+b\bar{\omega})$ and so must be of the form $a^2+b^2-ab = n$

Work mod 3 to see that such a number cannot be of the form $3k-1$.

$N(2+0\omega) = 4$ and there are no elements of $\mathbb{Z}[\omega]$ with norm 2 so this element is prime. $N(3) = 9$ and there are elements with norm 3. For example $3 = (2+\omega)(1+\omega)$.

[In fact the primes in $\mathbb{Z}[\omega]$ are primes in $\mathbb{Z}$ of the form $3k-1$ or 2 multiplied by a unit or elements whose norm is a prime (which will be of the form $3k+1$.]

35 The squares modulo 8 are 0, 1, 4 and one cannot make up 7 (mod 8) using less than 4 of them.

The smallest counterexample is $63 = 3 \times 21 = (1+1+1) \times (16+4+1)$

Representation as sums of four squares is <u>not</u> unique even for primes: $13 = 4+4+4+1 = 9+4+0+0$

Specifying <u>non-zero</u> squares you need to go a little further: $31 = 25+4+1+1 = 9+9+9+4$.

36 Using Gauss's theorem: 18, 54 have primitives; 12, 42, 266 do not.

$4k+2$ has a primitive for $k \leq 6$ but $30 = 2 \times 3 \times 5$ does not have a primitive

$\phi(10) = 4$ and $\phi(4) = 2$ so 10 has two primitives : 3 and 7.

$\phi(250) = 100$ and $\phi(100) = \phi(4) \times \phi(25) = 40$ so there are 40 primitives for 250.

Verifying that 3 is a primitive involves showing that the order of 3 in U_{250} is 100 and so that $3^k \neq 1 \mod 250$ for $k = 20, 50$.
$3^5 = -7$. So $3^{10} = 49 \Rightarrow 3^{20} = 151$ and $3^{50} = -1$ and so 3 is a primitive.

To find other primitives, take 3^k where $k, 100$ are coprime. e.g. $3^3 = 27$, $3^7 = 187$, $3^9 = 183$, $3^{11} = 147, \ldots$
[13, 17, 23, 33, ... are also primitives]

Working mod 5, $7 = 2$ which is a primitive for 5.
Working mod 25, $7^2 = -1$ and so $7^4 = 1$ but $\phi(25) = 20$ so 7 is not a primitive for 25.
To show that 2 is a primitive for 25, you need to verify that $2^k \neq 1 \mod 25$ for $k = 4, 10$. $2^4 = 16$ and $2^{10} = 1024 = -1 \mod 25$. So 2 is a primitive for both 5 and 25.

The only other primitive for 5 is 3 and it is easy to check that 3 is a primitive for 10, 25 and 50.

37 a) $133 = 7\times 19 \Rightarrow \left(\frac{133}{577}\right) = \left(\frac{7}{577}\right)\left(\frac{19}{577}\right) =$

$+\left(\frac{577}{7}\right)\left(\frac{577}{19}\right) = \left(\frac{3}{7}\right)\left(\frac{7}{19}\right) = -1\times -\left(\frac{19}{7}\right) = +\left(\frac{5}{7}\right) = -1$

$123 = 3\times 41 \Rightarrow \left(\frac{123}{4567}\right) = \left(\frac{3}{4567}\right)\left(\frac{41}{4567}\right) = -\left(\frac{4567}{3}\right)\left(\frac{4567}{41}\right)$

$= -\left(\frac{1}{3}\right)\left(\frac{16}{41}\right) = -1.1 = -1$

$209 = 11\times 19 \Rightarrow \left(\frac{209}{409}\right) = \left(\frac{11}{409}\right)\left(\frac{19}{409}\right) = \left(\frac{409}{11}\right)\left(\frac{409}{19}\right) =$

$\left(\frac{2}{11}\right)\left(\frac{10}{19}\right) = -1.\left(\frac{2}{19}\right)\left(\frac{5}{19}\right) = -1.-1.\left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = 1.$

b) $630 = 2\times 3^2\times 5\times 7$ and so n has a square root mod 630 iff n has a root mod 2, 3, 5, 7.
There are (resp) 2, 3, 4 numbers with roots mod 2, 5, 7 (including 0) and 4 modulo 9.
Hence there are 96 numbers with roots mod 630.

Obviously, 25 of these are: $1^2=1, 2^2=4, \ldots, 25^2=625$.
Others, like 46, 70, 85, ... are harder to spot.

c) If $N \equiv 0 \bmod q$ then $2 = (p_1 \ldots p_m)^2$ and so is a qr mod q. Hence q is of the form $\pm 1 \bmod 8$.
If all the prime divisors of N were of the

form $8k+1$ then N would be of this form also.
Hence N has a divisor of the form $8k-1$.
If $p_1, \dots, p_m$ were all the primes of the form $8k-1$ we would get a contradiction and so there must be infinitely many primes of this form.

d) Start by finding when -2 is a qr mod p.
$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ and looking at the cases $\pm 1, \pm 3$ mod 8 this is $+1$ if $p = \pm 3$ mod 8.
Now the proof works just as in the last case.

38. The quadratic residues mod 5 are 1, 4.
$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ by LQR and this is 1 if
$p = \pm 1$ mod 5

The qr mod 7 are 1, 4, 2 ; qnr are 3, 5, 6
$\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$ if $p = 1 \pmod 4$ and $\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$ if $p = 3 \pmod 4$. You can sort all this out working mod 28 : 7 is a qr mod p if p is
$1, 3, 9, 13, 19, 27 \pmod{28}$

$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$. $\left(\frac{3}{p}\right) = 1$ if $p = \pm 1 \bmod 12$
and $\left(\frac{-1}{p}\right) = (-1)^q$ where $q = \frac{1}{2}(p-1)$.

Then if $p = 6k+1$ then $q = 3k$ and so
if k is odd $(-1)^q = -1$ and $\left(\frac{3}{p}\right) = -1$;
if k is even $(-1)^q = +1$ and $\left(\frac{3}{p}\right) = +1$
and so $\left(\frac{-3}{p}\right) = 1$.

If $p = 6k-1$ then $q = 3k-1$ and so
if k is odd $(-1)^q = +1$ and $\left(\frac{3}{p}\right) = -1$;
if k is even $(-1)^q = -1$ and $\left(\frac{3}{p}\right) = +1$
and so $\left(\frac{-3}{p}\right) = -1$.

39 $\left(\frac{21}{55}\right) = \left(\frac{3}{5}\right)\left(\frac{7}{5}\right)\left(\frac{3}{11}\right)\left(\frac{7}{11}\right) = -1 . -1 . +1 . -1 = -1$

$$\left(\frac{17}{217}\right) = \left(\frac{17}{7}\right)\left(\frac{17}{31}\right) = \left(\frac{3}{7}\right)\left(\frac{31}{17}\right) = -\left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = -1.-1 = 1$$

$$\left(\frac{269}{889}\right) = \left(\frac{269}{7}\right)\left(\frac{269}{127}\right) = \left(\frac{3}{7}\right)\left(\frac{15}{127}\right) = -\left(\frac{3}{127}\right)\left(\frac{5}{127}\right) =$$
$$+\left(\frac{127}{3}\right)\left(\frac{127}{5}\right) = \left(\frac{1}{3}\right)\left(\frac{2}{5}\right) = 1.-1 = -1.$$

a has a square root mod b iff it has a square root modulo each prime power which divides b.
If $b = p_1^{s_1} \cdots p_k^{s_k}$ then $\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{s_1} \cdots \left(\frac{a}{p_k}\right)^{s_k}$

and if this product is -1 then one of the factors is -1 and so a does not have a square root modulo this prime.

You can see, however, that just because the product is $+1$ this does not guarantee that each factor is $+1$ which is why the converse fails.

40 Let $p = 2^{16}+1$. Then $|\mathbb{Z}_p - \{0\}| = 2^{16}$ and so every element has order a power of 2. By Euler's criterion, an element a is a quadratic non-residue iff $a^q = -1$ and then a will have order $p-1$ and will be a generator.

To prove that 75 is a non-residue, note that it is enough to prove that 3 is a non-residue since $75 = 5^2 \times 3$.

Since $p = 5 \bmod 12$ this follows from the result in lectures.

41 Use your calculator to get : $[0;1,6,2]$, $[0;1,1,22]$ and $[0;1,16,2]$.

$\frac{e-1}{e+1}$ has the expansion $[0;2,6,10,14,18,\ldots]$ and $\frac{\sqrt{e}-1}{\sqrt{e}+1}$ has expansion $[0;4,12,20,28,\ldots]$. Both these were discovered by Euler.

42 a) Starting from $[2;1,2,1,1,4,1,1,6,\ldots]=e$ gives $\frac{2}{1}, \frac{3}{1}, \frac{2\times3+2}{2\times1+1}=\frac{8}{3}, \frac{11}{4}, \frac{19}{7}, \frac{4\times19+11}{4\times7+4}=\frac{87}{32}, \frac{106}{39}, \frac{193}{71}, \ldots$ In fact $\frac{2721}{1001} = 2.7182817\ldots$ correct to 6 d.p.

b) $\sqrt{2} = [1;2,2,2,\ldots]$ gives $\frac{1}{1}, \frac{3}{2}, \frac{2\times3+1}{2\times2+1}=\frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{99}{70}, \frac{239}{169}, \ldots$ Note that $\frac{99^2}{70^2} = \frac{9801}{4900} \doteq 2.0002\ldots$

c) $\sqrt{3} = [1;1,2,1,2,\ldots]$ and one finds $\frac{265}{153}$ and $\frac{1351}{780}$ as (resp) C_8 and C_{11}.

43. $\sqrt{17} = [4;8,8,\ldots]$ (period 1)

$\lambda = \lambda_0 = \sqrt{17}$. $a_0 = [\lambda_0] = 4 \Rightarrow$

$$\lambda_1 = \frac{1}{\sqrt{17}-4} = \frac{\sqrt{17}+4}{1} \Rightarrow a_1 = [\lambda_1] = 8$$

$$\Rightarrow \lambda_2 = \frac{1}{\sqrt{17}-4} = \lambda_1$$ and so we have periodicity.

$$\sqrt{15} = [3;1,6,1,6,\ldots] \quad (\text{period} = 2)$$

$\lambda = \lambda_0 = \sqrt{15}$. $\quad a_0 = [\lambda_0] = 3 \Rightarrow$

$$\lambda_1 = \frac{1}{\sqrt{15}-3} = \frac{\sqrt{15}+3}{6} \Rightarrow a_1 = [\lambda_1] = 1 \Rightarrow$$

$$\lambda_2 = \frac{6}{\sqrt{15}-3} = \frac{6}{6}(\sqrt{15}+3) \Rightarrow a_2 = [\lambda_2] = 6 \Rightarrow$$

$\lambda_3 = \frac{1}{\sqrt{15}-3} = \lambda_1$ and we have periodicity.

Applying Newton's method to $x^2-2=0$ with $x_1 = 1$ and $x_{n+1} = \frac{x_n^2+2}{2x_n}$ gives the sequence $\left(1, \frac{3}{2}, \frac{17}{12}, \frac{577}{408}, \ldots\right)$ These 4 terms are (resp) C_0, C_1, C_3, C_7 among the convergents of the continued fraction.

The next term in Newton's approximation is $\frac{665857}{470832}$ which is C_{15} — telling you something about the convergence of the two methods.

44 If $\lambda = [0; \overline{1,4}]$ then $\lambda = 0 + \frac{1}{1+\frac{1}{4+\lambda}} \Rightarrow$

$\lambda = \frac{4+\lambda}{5+\lambda} \Rightarrow \lambda^2+4\lambda-4=0 \Rightarrow \lambda = \sqrt{8}-2$.

If $\lambda = [0; \overline{1,2,3}]$ then $\lambda = \frac{1}{1+\frac{1}{2+\frac{1}{3+\lambda}}}$

$\Rightarrow \lambda = \frac{7+2\lambda}{10+3\lambda} \Rightarrow 3\lambda^2+8\lambda-7=0 \Rightarrow \lambda = \frac{\sqrt{85}-8}{6}$.

45 a) $\sqrt{6} = [2; \overline{2,4}]$ with $k=2$.

Convergents are $\frac{2}{1}, \frac{5}{2}, \frac{4\times5+2}{4\times2+1} = \frac{22}{9}, \frac{2\times22+5}{2\times9+2} = \frac{49}{20}, \ldots$

and so solutions of Pell's equation are $(5,2), (49,20), \ldots$

Note that one could "spot" the first one (or calculate C_1) and then deduce others by calculation in $\mathbb{Z}[\sqrt{6}]$.

$\sqrt{15} = [3; \overline{1,6}]$ with $k=2$.

Convergents are : $\frac{3}{1}, \frac{4}{1}, \frac{6\times4+3}{6\times1+1} = \frac{27}{7}, \frac{31}{8}, \ldots \Rightarrow$

solutions $(4,1), (31,8), \ldots$ for Pell's equation.

b) Work in $\mathbb{Z}[\sqrt{d}]$ with norm $N(a+b\sqrt{d}) = a^2-b^2d$

Then if $N(a+b\sqrt{d})=1$ then $N((a+b\sqrt{d})^2)=1 \Rightarrow$

$N(a^2+b^2d+2ab\sqrt{d})=1 \Rightarrow (a+bb^2, 2ab)$ is a solution. If $N(A+B\sqrt{d})=1$ also then the product $(a+b\sqrt{d})(A+B\sqrt{d})$ has norm 1 giving the next result.

The final result follows from $N(u)=k_1, N(v)=k_2$ $\Rightarrow N(uv)= k_1k_2$.

Brahmagupta didn't prove it this way!

46 If $x^2-31y^2=-1$ then work mod 31 $\Rightarrow$ $x^2=-1$. But, by Euler's criterion, $\left(\frac{-1}{31}\right)=(-1)^{15}$ and so -1 is not a quadratic residue.

Solving $x^2-31y^2=1$ involves finding the $(k-1)$st convergent of the continued fraction for $\sqrt{31}$. This is $[5; \overline{1,1,3,5,3,1,1,10}]$ which my calculator can't handle (though MAPLE can)! The 7th convergent is 1520/273 so calculating it by hand needs serious determination!

$5x+3y=104$. $-1.5+2.3=1$ and $3\lambda.5-5\lambda.3=0$ $\Rightarrow -104.5+208.3=104 \Rightarrow x=3\lambda-104, y=-5\lambda+208$ is a general solution. "Small" positive solutions are $x=1, y=33$; $x=22, y=2, \ldots$

47 The largest integer not expressible as $5x+17y$ with $x,y\geqslant 0$ is 63. (Note that one can get 64, 65, 66, 67, 68 and once you have a "run of 5" you can get everything bigger.) If a,b are coprime the largest number you can't get is $(a-1)(b-1)-1$.