1.1.10: Let’s look at the first word. If I shift forward by 1 or 2 steps, I get nonsense. But if I shift forward by 3, I get “BUT”. This looks promising, so let’s try a forward shift of 3:

“BUT THIS EXAMPLE IS LESS EASY”.

1.2.15; Let’s write the number N as def, where f is the ones-place, e is the tens place and d is all the digits to the left of the e and f. (So, for example, if N =123456789, then f=9, e=8, and d=1234567.) Then N = 100d+10e+f. Since 100d%100 =0, we see that N%100=10e+f%100, and 10e+f is just the two digit number made up of the tens place and the ones place.

1.2.17. We are given that r is the reduction of N mod m. That means the N=qm+r, where q is some integer and 0<r<m. Then –N=–qm–r =–(q+1)m+(m–r). Since we are given that r≠0, we see that 0<m–r<m; hence m–r is the reduction of −N mod m.

1.2.19. We want to find an integer, let’s call it cd, such that 87(cd)%100 =1. (Here I mean that that the ten’s digit is c and the unit digit is d). Note that the number 87(cd) must end in 1, and so d must be 3. Let’s set up the multiplication:

```
  87
× 3
  261
```

It’s clear that the right-most “?” has to be 4, since the ten’s digit of the answer must be 0. So 7 times c must end in 4, so c must be 2. Hence the answer is 23.

Let’s check (87)(23)=2001, and 2001%100 = 1.

It’s OK to do this problem by brute force (but note how a little thinking can save a lot of force) or by using the Euclidean Algorithm.

1.5.8. Notice that 3n ≡ −1 mod 3n+1, so (−3)n%3n+1 = 1. Hence −3 is a multiplicative inverse of n. However −3 is not a non-negative value less than 3n+1, so to get a proper answer we must add 3n+1 to −3 to get 3n−2. So the answer is that the mult. inverse of n is 3n−2.

Challenge: Find q such that (n)(3n−2) =q(3n+1) + 1.

You need to justify your answer by general mathematical reasoning, as above. Using several special cases to guess the correct answer is good problem-solving strategy, but you still must verify that your answer is correct.
1.6.9: \(2^5 = 32\) and \(32 \equiv (-1) \pmod{11}\). Then \(2^{10} \equiv (2^5)^2 \equiv (-1)^2 \equiv 1 \pmod{11}\). Hence \(2^{1000} \equiv (2^{10})^{100} \equiv 1 \pmod{11}\).

There are many reasonable ways to do this problem. The unreasonable way is to attempt to calculate \(2^{1000}\) and then reduce mod 11.

1.6.14. Well, 1, and \(-1\) (that is 104) certainly work. Also 29, 34, 41, 64, 71, and 76 work. Later we will find a more systematic way of doing this problem, and we will learn that if \(n\) is a prime, then there are only two solutions to \(x^2 \equiv 1 \pmod{n}\).

1.6.20: If \(n\) has decimal digits \(a_k, a_{k-1}, \ldots, a_1, a_0\), then \(n=10^k a_k + 10^{k-1} a_{k-1} + \ldots + 10 a_1 + a_0\). Note that \(10 \equiv 1 \pmod{9}\), so \(10^i \equiv 1 \pmod{9}\) for all non-negative integers \(i\). Hence \(10^i a_i \equiv a_i \pmod{9}\); taking sums we get \(N \equiv a_k + a_{k-1} + \ldots + a_1 + a_0 \pmod{9}\).

1.6.22. 123456789123456789 \% 9 = 0, but 28958998683279996179682996625361999 \% 9 = 8. So the two sides can’t be equal.

1.7.7. A multiplicative inverse of 11 mod 26 is 19. (It is OK just to state this.) Hence if \(y=11x+5 \pmod{26}\), then \(y-5=11x \pmod{26}\) and \(19(y-5) \equiv x \pmod{26}\). Hence the decoding function is \(D(y)=19(y-5) \pmod{26}\). Putting this in standard form, we get \(D(y)=19y-95 \equiv 19y+9 \pmod{26}\). So the answer is \(D(y)=19y+9 \pmod{26}\).

Let’s check: \(D(E(x)) \equiv D(11x+5) \equiv 19(11x+5)+9 \equiv 19(11)x+95+9 \equiv x\).

1.7.14: \(3a+b=5 \pmod{26}\) and \(6a+b=7 \pmod{26}\). Subtracting, we get \(3a=2 \pmod{26}\). A mult inv of 3 is 9, so \(a=18\). Then using \(3a+b=5 \pmod{26}\) with \(a=18\), we get \((3)(18)+b=5 \pmod{26}\), so \(2+b=5 \pmod{26}\). So \(b=3\). Hence the answer is \(a=18\) and \(b=3\).

Check: If \(E(x)=18a+3 \pmod{26}\), then \(E(3)=(18)(3)+3 \equiv 5 \pmod{26}\) and \(E(6)=(18)(6)+3 \equiv 7 \pmod{26}\).

1.7.19: We are given \(3a+b=5 \pmod{26}\) and \(5a+b=7 \pmod{26}\). Subtracting, we get \(2a=2 \pmod{26}\). Note that 2 does not have a mult.inv mod 26. One solution of \(2a=2 \pmod{26}\) is \(a=1\), but there is another solution, namely \(a=14\). So the two possibilities for \(a\) are 1 and 14.

If \(a=1\), then \(3a+b=5 \pmod{26}\) becomes \(3+b=5 \pmod{26}\), so \(b=2\). If \(a=14\), then \(3a+b=5 \pmod{26}\) becomes \(42+b=5 \pmod{26}\), so \(b=(5-42) \equiv -37 \equiv 15 \pmod{26}\). So the other solution is \(E(x)=14x+15\).
Hence the two solutions are $E(x)=x+2\%26$ and $E(x)=14x+15\%26$. You can check that these work.

If you only had the first solution, you get only one point out of 10, since the core of the problem is that there are two solutions. If you somehow used the multiplicative inverse of 2 (which does not exist), you get zero.

2.1.12: We can choose the first subset in $\binom{8}{3}$ ways. Then we can choose the second subset in $\binom{5}{3}$ ways. But we have double-counted, since we could switch the labels “first subset” and “second subset” and still have the same collection of subsets. So the answer is

$$\binom{8}{3}\binom{5}{3}/2 = [(8)(7)(6)/(6)][(5)(4)(3)/6]/2 = 280$$

If you forgot to include the “2” in the denominator of your formula, you lose half credit for this problem. You may think this is harsh, but an identical problem is worked out on Page 23.

2.2.3: $Pr(\text{more heads than tails}) = Pr(4\text{heads})+Pr(5\text{heads})+Pr(6\text{heads}) = [C(6,4)+C(6,5)+C(6,6)]/2^6 = [15+6+1]/2^6 = 22/64 = 11/32$.

ALT: $Pr(3\text{heads})=C(6,3)/2^6=20/64$, so $Pr(\text{other than 3 heads}) = 44/64$. Half of this will be more heads than tails and half will more tails than heard, so $Pr(\text{more heads than tails})=22/64=11/32$.

2.2.6: With replacement. $Pr(\text{first red})=0.3; Pr(\text{second red})=0.3$, so $Pr(\text{both red}) = (0.3)(0.3) = 0.09$.

Without replacement: $Pr(\text{first red})=3/10; Pr(\text{second red, given first is red}) = 2/9$, so $Pr(\text{both are red}) = (3/10)(2/9)=6/90=1/15$.

ALT: (Without rep). We pick two balls out of 10. This can be done in $\binom{10}{2}$ ways. But in how many ways can we chose two red? In $\binom{3}{2}$ ways. So the answer is $\binom{3}{2}/\binom{10}{2} = [((3)(2))/(10)(9)] = 1/15$.

2.2.12: Solution 1: Use the Proposition on Page 30: $N=365$, so $(2\ln 2)^{1/2}N^{1/2} \approx 22.49$; hence if $n=23$, the Prob is greater than $1/2$ that at least two have the same birthday.

Solution 2: If we have $n$ people, the probability that they will all have distinct birthdays is $(364/365)(363/365)(362/365)\ldots((365-n+1)/365))$. When $n=23$, this is $(364/365)(363/365)\ldots(343/365)=0.492702766$. Hence the prob that two or more will have the same birthday is approx.. $1-.49 = .51$. 