

Exercise 6 on page 41 should ask for an exponentiation program. Here is an exponentiation program in UBASIC:

```
100 print "what are a, b, c"
110 input a, b, c
120 x = 1
130 y = a
140 z = b
150 while z > 0
160 q = 0
170 r = z
180 while r >= 2
182 k = 1
184 while r >= 4*k
186 k = 2*k
188 wend
190 r = r - 2*k
200 q = q + k
210 wend
220 if r = 0 then z = q else z = z - 1
230 if r = 0 then p = y*y else p = x*y
240 while p >= c
242 k = 1
244 while p >= 2*k*c
246 k = 2*k
248 wend
250 p = p - k*c
260 wend
270 if r = 0 then y = p else x = p
280 wend
290 print x, "is", a, "to the power", b, "mod", c
```

Revision on pages 34-35:

Replace the five sentences that begin "Since the greatest common ..." on the third line from the bottom of page 34 and end " $p_1 p_2 \cdots p_m = p_1 q_2 \cdots q_n$ " on line 7 of page 35 with:

Since  $p_1$  divides the product  $q_1 q_2 \cdots q_n$  and is prime, the proposition above implies that  $p_1$  divides at least one of the factors  $q_i$ . Rearrange the factors, if necessary, to make  $p_1$  divide  $q_1$ . Since  $q_1$  is prime and  $p_1 > 1$ ,  $q_1$  must be equal to  $p_1$ , and the original equation becomes  $p_1 p_2 \cdots p_m = p_1 q_2 \cdots q_n$ .

(The proof of the theorem was written first. When the opening of the chapter was revised to include the proposition, the proof should have been simplified in this way.)

**Errata**

In the second line of the Proposition on page 73, omit the word “then.”