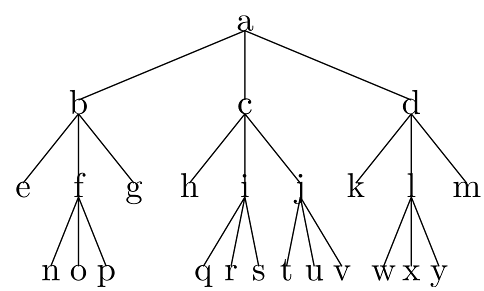
R11.2 Use the divide-and-conquer algorithm (Karatsuba) from section 11.2 to compute

$$1011\ 0011 \cdot 1011\ 1010$$

in binary.

Solution. We use the following computation tree.



We use the version of the recursion formula given in class:

$$(x_h 2^{n/2} + x_l)\cdot(y_h 2^{n/2} + y_l) = (x_h \cdot y_h)2^n + [(x_h + x_l)\cdot(y_h + y_l) - x_h \cdot y_h - x_l \cdot y_l]\, 2^{n/2} + (x_l \cdot y_l)$$

- a = 1011 0011 · 1011 1010
  = b · 1 0000 0000 + (c - b - d) 1 0000 + d = 1000 0010 0000 1110
- b = 1011 · 1011 = e · 1 0000 + (f - e - g) 100 + g = 111 1001
- c = 1110 · 1 0101 = h · 100 0000 + (i - h - j) 1000 + j = 1 0010 0110
- d = 0011 · 1010 = k · 1 0000 + (l - k - m) 100 + m = 1 1110
- e = 10 · 10 = 100
- f = 101 · 101 = n · 1 0000 + (o - n - p) 100 + p = 1 1001
- g = 11 · 11 = 1001
- h = 1 · 10 = 10
- i = 111 · 111 = q · 1 0000 + (r - q - s) 100 + s = 11 0001
- j = 110 · 101 = t · 1 0000 + (u - t - v) 100 + v = 1 1110
- k = 00 · 10 = 0
- l = 11 · 100 = w · 1 0000 + (x - w - y) 100 + y = 1100
- m = 11 · 10 = 110
- n = 1 · 1 = 1
- o = 10 · 10 = 100
- p = 01 · 01 = 1
- q = 1 · 1 = 1
- r = 100 · 100 = 1 0000
- s = 11 · 11 = 1001
- t = 1 · 1 = 1
- u = 11 · 10 = 110
- v = 10 · 01 = 10
- w = 0 · 1 = 0
- x = 11 · 1 = 11
- y = 11 · 0 = 0

•

R11.4 Describe a method performing only three real-number multiplications to compute the product $a + bi$ and $c + di$.

Solution. It is easy to verify that the following equation is true.

$$(a + bi)(c + di) = (ac - bd) + [(a + b)(c + d) - ac - bd]\, i.$$

So to perform the product of $a+bi$ and $c+di$, compute the 3 real-number multiplications

$$p = ac, \quad q = bd, \quad r = (a + b)(c + d)$$

and combine them as $p - q + (r - p - q)i$. •

R24.5 Show the execution of method FastExponentiation(5, 12, 13).

Solution. We are computing $r = 5^p \mod 13$ where $p = 12$.

p	12	6	3	1	0
r	1	12	8	5	1

•

C24.6 Supppose that Alice wants to send Bob a message M that is the price she is willing to pay for his old bike. Here, M is an integer in binary. She uses RSA to encrypt M to produce the ciphertext C using Bob's public key and sends it to Bob. Unfortunately Eve has intercepted C before it gets to Bob. Explain how Eve can use Bob's public key to alter the ciphertext C to change it into C' so that if she sends C' to Bob, then, after Bob had decrypted C', he will get a plaintext that is twice the value of M.

Solution. Using the notation from the book, suppose that Bob's public key is e, his private key d, and that the two primes chosen are p and q. Let $n = pq$. This means that for any x, these numbers have the property that

$$x^{ed} \equiv x \mod n.$$

Then Alice got the ciphertext her message M by doing

$$C \equiv M^e \mod n.$$

So if Eve takes C and modifies it by multiplying by $2^e \mod n$,

$$C' \equiv 2^e \cdot C \mod n,$$

then when Bob decrypts this message C', he will get

$$(C')^d \mod n \equiv (2M)^{ed} \mod n \equiv 2M.$$

•