1. (i) 2^{k-1}, $2^k - 1$

   (ii) $k = \lfloor \lg x \rfloor + 1$

   (iii) $2k$

2. The code below is called with x, y, and n each having $k \geq 2$ bits.

   (i) $2k$

   (ii) k (since the answer is at most $n - 1$).

3. ```
   313 = 5*61 + 8
    61 = 7* 8 + 5
     8 = 1* 5 + 3
     5 = 1* 3 + 2
     3 = 1* 2 + 1    <-- gcd is 1
     2 = 2* 1 + 0

     1 = 3 - 1*2  = 3 - 1*(5 - 1*3) = 2*3 - 1*5
       = 2*(8 - 1*5) - 1*5  = 2*8 - 3*5
       = 2*8 - 3*(61 - 7*8) = 23*8 - 3*61
       = 23*(313 - 5*61) - 3*61 = 23*313 - 118*61
   ```

   (iii) 1 is a linear combination of 313 and 61, and 1 divides both 313 and 61, so the gcd of 313 and 61 must divide 1, so it must be at most 1. But the gcd of integers is at least 1. So the gcd of the two numbers must be exactly 1, so our answer is correct.

   (iv) $61 * (-118) = 1 - 23 * 313$, so $61^{-1} (\text{mod } 313) = -118 = 313 - 118 = 195$

   (v) both are prime. it depends, but in general (as the numbers get large) there will be less arithmetic with (i) than with (v).

4. ```
   2 1
   3 2
   4 2
   5 4
   6 2
   7 6
   8 4
   9 6
   10 4
   11 10
   12 4
   13 12
   14 6
   15 8
   16 8
   17 16
   18 6
   19 18
   ```

5. (i) 220417 (ii) composite (iii) 1 (iv) probably prime (v) 1 (vi) probably prime