(1) DPV Problem 1.7.

Suppose x is n bits long and y is m bits long.

Answer: $O(m \cdot (m+n))$. Justification: There are m recursive calls because in each call y is halved - that is its number of bits is decreased by one. In each recursive call we have the division by 2, the odd/even test, and the multiplication by 2, and possibly the addition of x to $2z$. The addition is of an n bit number (x) to a number that is no more than $m+n+1$ bits ($2z$). So each step is $O(m+n)$. Hence, the total complexity is $m \cdot O(m+n) = O(m \cdot (m+n))$.

(2) DPV Problem 1.10.

$a \equiv b \pmod{N}$ means that $a - b = u \cdot N$ for some integer u. $M|N$ means that $N = k \cdot M$ for some integer k. Hence, $a - b = u \cdot k \cdot M = (u \cdot k) \cdot M$. Therefore, $a \equiv b \pmod{M}$.

(3)

(a) Suppose p is prime, $\gcd(a,p) = 1$, $k \geq 0$, and $k' = (k \bmod (p-1))$. **Claim:** $a^k \cong a^{k'} \bmod p$. **Proof:** First note that $k = q \cdot (p-1) + k'$ for some integer q. By Fermat's Little Lemma, $a^{p-1} \cong 1 \bmod (p-1)$. Hence, $a^k \cong$

$$a^{q\cdot(p-1)+k'} \;\cong\; (a^{(p-1)})^q \cdot a^{k'} \;\cong\; (1)^q \cdot a^{k'} \;\cong\; 1 \cdot a^{k'} \;\cong\; a^{k'} \bmod p.$$

(b) $2^{1678923} \bmod 137 = 2^{1678923 \bmod 136} \bmod 137 = 2^3 \bmod 137 = 8$.

(4) DPV Problem 1.19. Recall $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$, for each $n \geq 0$.

(a) $F_{n+2} = F_{n+1} + F_n \implies F_{n+2} - F_{n+1} = F_n \implies (F_{n+2} - F_{n+1}) \bmod F_{n+1} = F_n \bmod F_{n+1} = 0$. Note, $(F_{n+2} - F_{n+1}) \bmod F_{n+1} = F_{n+2} \bmod F_{n+1}$, and, since $F_n < F_{n+1}$, $F_n \bmod F_{n+1} = F_n$. Hence, $F_{n+2} \bmod F_{n+1} = F_n$.

(b) Claim: For each $n > 0$, $\gcd(F_{n+1}, F_n) = 1$. **Proof by induction:**

Base case: $n = 1$. Note: $\gcd(F_2, F_1) = \gcd(2,1) = 1$.

Induction step: IH: $\gcd(F_{n+1}, F_n) = 1$.

GOAL: Show $\gcd(F_{n+2}, F_{n+1}) = 1$.

$$\begin{aligned}
\gcd(F_{n+2}, F_{n+1}) &= \gcd(F_{n+1}, (F_{n+2} \bmod F_{n+1})) && \text{(by Euclid's Rule)}\\
&= \gcd(F_{n+1}, F_n) && \text{(by part (a))}\\
&= 1 && \text{(by the IH).}
\end{aligned}$$

(5) DPV Problem 1.20. We can use the following functions from `rsa.hs` for this problem:

```
xgcd a b
    = if (b==0)
      then (1,0,a)
      else (y',x'-y'*q,d)
           where  (q,r)     = divMod a b -- a = q*b+r & 0<=r<b
                  (x',y',d) = xgcd b r

invert a n = let (x,y,d) = xgcd a n
             in if (d/=1) then 0 else x `mod` n
```

Here are the answers: $4 = 20^{-1} \pmod{79}$; $32 = 2^{-1} \pmod{63}$; $14 = 5^{-1} \pmod{23}$; and $21^{-1} \pmod{91}$ is undefined since $\gcd(21,91) = 7$.

(6) DPV Problem 1.27.

$$\begin{aligned}
e^{-1} \bmod ((p-1)\cdot(q-1)) = 3^{-1} \bmod (16 \cdot 22) &= 235.\\
m^e \bmod (p \cdot q) = 41^3 \bmod 391 &= 105.\\
(m^e)^d \bmod (p \cdot q) = 105^{235} \bmod 391 &= 41. \quad \textit{(check)}
\end{aligned}$$