CS1231 TUTORIAL 7

1. $\sqrt{113} < 11$ and the primes less than 11 are 2, 3, 5, 7. None of these is a divisor of 107 or 113. Thus they are both primes.

2. If $d \mid n$ and $\sqrt{n} < d \leq n$, then $d' \mid n$ where $d' = n/d$ and $1 \leq d' < \sqrt{n}$. Thus each positive divisor of n which is less than $\sqrt{n}$ can be paired up with a positive divisor $> \sqrt{n}$. Hence the number of divisors of n that are different from $\sqrt{n}$ is even. $\sqrt{n}$ itself is a divisor iff n is a perfect square. Thus n is a perfect square iff it has an odd number of positive divisors.

3. $(101000001)_2$.

4. It is $1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 351$.

5. $175627 = 10976 \cdot 16 + 11$

$10976 = 686 \cdot 16 + 0$

$686 = 42 \cdot 16 + 14$

$42 = 2 \cdot 16 + 10$

$2 = 0 \cdot 16 + 2$

$175627 = (2AE0B)_{16}$.

6. $644 = (1010000100)_2 = 512 + 128 + 4$.

$$11^2 \textbf{ Mod } 645 = 121 \qquad 11^4 \textbf{ Mod } 645 = 121^2 \textbf{ Mod } 645 = 451$$
$$11^8 \textbf{ Mod } 645 = 451^2 \textbf{ Mod } 645 = 226 \qquad 11^{16} \textbf{ Mod } 645 = 226^2 \textbf{ Mod } 645 = 121$$
$$11^{32} \textbf{ Mod } 645 = 451 \qquad 11^{64} \textbf{ Mod } 645 = 226 \qquad 11^{128} \textbf{ Mod } 645 = 121$$
$$11^{256} \textbf{ Mod } 645 = 451 \qquad 11^{512} \textbf{ Mod } 645 = 226$$

Thus 11^{644} **Mod** $645 = 226 \cdot 121 \cdot 451$ **Mod** $645 = 1$.

7. 14039 **Mod** 1529 = 278, 1529 **Mod** 278 = 139, 278 **Mod** 139 = 0. Therefore $\gcd(14039, 1529) = 139$.

1529 **Div** 278 = 5 and 14039 **Div** 1529 = 9. Thus $1529 = 5 \cdot 278 + 139$ and $14039 = 9 \cdot 1529 + 278$. Hence

$$139 = 1529 - 5 \cdot 278 = 1529 - 5(14039 - 9 \cdot 1529) = 46 \cdot 1529 - 5 \cdot 14039$$