18.781 Solutions to Problem Set 3

1. It's enough to solve the congruence mod 11 and mod 13, and then combine the solutions by Chinese Remainder Theorem. Now $x^3 - 9x^2 + 23x - 15$ factors as $(x-1)(x-3)(x-5)$, so solutions mod 11 or mod 13 are $1, 3, 5$ in each case. To combine, we first need x, y such that $13x + 11y = 1$. For instance $x = -5, y = 6$ works. (We can find x, y by Euclidean algorithm). So if we have a solution a mod 11 and a solution b mod 13 then the Chinese Remainder Theorem recipe tells us that

$$(-5)(13)a + (6)(11)b = -65a + 66b$$

is a solution mod 143. Running this over $a \in \{1, 3, 5\}$ and $b \in \{1, 3, 5\}$ we get 9 solutions: 1, 3, 5, 14, 16, 27, 122, 133, 135.

2. We just need to compute these expressions mod 4 and mod 25, and then combine using CRT. Note that $(1)(25) + (-6)(4) = 1$, so if $x \equiv a$ mod 4 and $x \equiv b$ mod 25 then $x \equiv 25a - 24b \pmod{100}$.

   For 2^{100}: We have $2^{100} \equiv 0 \pmod 4$ and $2^{100} = 2^{5\phi(25)} \equiv 1 \pmod{25}$. So the last two digits are $25 \cdot 0 - 24 \cdot 1 \equiv 76$.

   For 3^{100}: We have $3^{100} = 3^{50\phi(4)} \equiv 1 \pmod 4$ and $3^{100} = 3^{5\phi(25)} \equiv 1 \pmod{25}$. So the last two digits are $25 \cdot 1 - 24 \cdot 1 \equiv 01$.

3. Let $m = \prod p_i^{e_i}$. By the CRT, we can simply find the number of solutions mod $p_i^{e_i}$ for each i and take the product. Now $x^2 \equiv x \pmod{p^e}$ means $p^e | x^2 - x = x(x-1)$. Since x and $x - 1$ are coprime, we have $p^e | x$ or $p^e | x - 1$. So $x \equiv 0, 1 \pmod{p^e}$ are the two solutions. Thus, for an arbitrary integer m, the number of solutions is 2^r where r is the number of distinct prime divisors of m.

4. (a) We need to show that $a^{560} \equiv 1$ mod 3, mod 11, and mod 17 for any a coprime to 561.
   Since a is coprime to 3, $a^2 \equiv 1 \pmod 3$, so $a^{560} = a^{2\cdot 280} \equiv 1 \pmod 3$.
   Since a is coprime to 11, $a^{10} \equiv 1 \pmod{11}$, so $a^{560} = a^{56\cdot 10} \equiv 1 \pmod{11}$.
   Since a is coprime to 17, $a^{16} \equiv 1 \pmod{17}$, so $a^{560} = a^{35\cdot 16} \equiv 1 \pmod{17}$.

   (b) Suppose $n = pq$ with p, q distinct primes satisfies property P. Then for all a coprime to p and q, we have $a^{pq-1} \equiv 1 \pmod p$ and $a^{pq-1} \equiv 1 \pmod q$.
   Assume, without loss of generality, that $p < q$. Then

$$\begin{aligned} a^{pq-1} &= a^{(q-1)p+p-1} \\ &= a^{(q-1)p} \cdot a^{p-1} \\ &\equiv 1^p \cdot a^{p-1} \pmod q. \end{aligned}$$

   Now for any x coprime to q, we can let a be the unique integer mod pq which satisfies $a \equiv x \pmod q$ and $a \equiv 1 \pmod p$, so that a is coprime to pq and thus $x^{p-1} \equiv 1 \pmod q$. However, because of the existence of a primitive root mod q, we know that $q - 1$ is the smallest positive integer such that $x^{q-1} \equiv 1 \pmod q$ for every x coprime to q. Since $p - 1 < q - 1$, we have a contradiction.

   (c) A sufficient condition is that $p-1 | pqr-1$. This implies that $qr \equiv 1 \pmod{p-1}, pr \equiv 1 \pmod{q-1}$, and $pq \equiv 1 \pmod{r-1}$. Using it to search we find the following numbers:

$$\begin{aligned}
561 &= 3 \cdot 11 \cdot 17 \\
1105 &= 5 \cdot 13 \cdot 17 \\
1729 &= 7 \cdot 13 \cdot 19 \\
2465 &= 5 \cdot 17 \cdot 29 \\
2821 &= 7 \cdot 13 \cdot 31 \\
6601 &= 7 \cdot 23 \cdot 41 \\
8911 &= 7 \cdot 19 \cdot 67 \\
10585 &= 5 \cdot 29 \cdot 73 \\
15841 &= 7 \cdot 31 \cdot 73 \\
29341 &= 13 \cdot 37 \cdot 61.
\end{aligned}$$

5. Yes. Pick distinct primes $p_1, \ldots, p_N$ and let x solve

$$\begin{aligned}
x &\equiv 0 \pmod{p_1^2} \\
x + 1 &\equiv 0 \pmod{p_2^2} \\
&\vdots \\
x + N - 1 &\equiv 0 \pmod{p_N^2}
\end{aligned}$$

   This has solutions mod $p_1^2 \cdots p_N^2$, by CRT. We can pick x positive. Then for each i, $x+i-1$ is divisible by p_i^2, and thus is not squarefree.

6. (a) You should find that the density is about 2/3.
   (b) You should find that the density is about 1/3.
   (c) The key difference is the Galois group, which is S_3 for (a) and $\mathbb{Z}/3\mathbb{Z}$ for (b). The reason for the distribution you see is a deep theorem in algebraic number theory called the Chebotarev density theorem. In terms of group theory, the main difference is that the number of permutations in S_3 with a fixed point is 4, leading to the fraction $4/6 = 2/3$, while the corresponding number for $A_3 = \{(1), (123), (132)\}$ is 1, leading to the fraction $1/3$.

18.781 Theory of Numbers
Spring 2012