Homework **28** Solutions

Problems

1. **We've seen that we can use Fermat's Theorem to test if a number is composite. If a number is prime, then it will alway's pass this "Fermat test." What if the number n is composite? What fraction of a that are relatively prime to n satisfy $a^{n-1} \equiv 1 \pmod{n}$? It turns out that there are some n so that *all* a have this property, yet n is composite! Such numbers are called *Carmichael numbers*.**

   The smallest Carmichael number is 561. In this problem we'll take a look at why 561 has no witnesses for the Fermat test.

   (a) **Find the factorization of 561.**

$$\begin{aligned} 561 &= 3 \cdot 187 \\ &= \boxed{3 \cdot 11 \cdot 17} \end{aligned}$$

   (b) **Find the factorization of 560.**

$$\begin{aligned} 560 &= 56 \cdot 10 \\ &= 8 \cdot 7 \cdot 10 \\ &= \boxed{2^4 \cdot 5 \cdot 7} \end{aligned}$$

   (c) **Now suppose that a is relatively prime to 561. Use the Chinese Remainder Theorem, and Fermat's Theorem to explain why $a^{560} \equiv 1 \pmod{561}$ (see Homework 24 for an example)**

   By the Chinese Remainder Theorem, it's enough to show that $a^{560} \equiv 1 \pmod{3}$ and $a^{560} \equiv 1 \pmod{11}$ and $a^{560} \equiv 1 \pmod{17}$. But 560 is divisible by $3-1$ and $11-1$ and $17-1$, so the result now follows from Fermat's Theorem.

   (d) (**Optional challenge**; you will not be graded on this part) Find the next Carmichael number.

   We note that the condition that n is a Carmichael number is the same as the condition that n is not divisible by any square and that for every prime p dividing n, $p-1$ divides $n-1$ (the reason for this is basically that given in the previous part of this problem).

   This implies that n must be odd. Otherwise, if n had any odd primes dividing it, then $p-1$ would be even and thus would not divide $n-1$, which would be odd. But the only other possibility would be n a power of 2, which is easily verified to not be a Carmichael number.

   Similarly, one can show that n must be divisible by at least three primes. Why? Suppose that $n = pq$ where $q > p$. Then $n - 1 = pq - 1 = (p+1) \cdot (q-1) + p - q$, so $q - p$ must be divisible by $q - 1$. This doesn't make sense, since $q - 1 > q - p > 0$.

   So, we can now just brute force check through triple products of odd primes.

   $105 = 3 \cdot 5 \cdot 7$ fails since 104 is not divisible by $6 = 7 - 1$.

   $165 = 3 \cdot 5 \cdot 11$ fails since 164 is not divisible by $10 = 11 - 1$.

   $195 = 3 \cdot 5 \cdot 13$ fails since 194 is not divisible by $12 = 13 - 1$.

   $255 = 3 \cdot 5 \cdot 17$ fails since 254 is not divisible by $4 = 5 - 1$.

   $231 = 3 \cdot 7 \cdot 11$ fails since 230 is not divisible by $6 = 7 - 1$.

   $273 = 3 \cdot 7 \cdot 13$ fails since 272 is not divisible by $6 = 7 - 1$.

$357 = 3 \cdot 7 \cdot 17$ fails since 356 is not divisible by $6 = 7 - 1$.

$429 = 3 \cdot 11 \cdot 13$ fails since 428 is not divisilble by $10 = 11 - 1$.

$561 = 3 \cdot 11 \cdot 17$ is the Carmichael number we already know of.

$663 = 3 \cdot 13 \cdot 17$ fails since 662 is not divisible by $12 = 13 - 1$.

$385 = 5 \cdot 7 \cdot 11$ fails since 384 is not divisible by $10 = 11 - 1$.

$455 = 5 \cdot 7 \cdot 13$ fails since 454 is not divisible by $6 = 7 - 1$.

$595 = 5 \cdot 7 \cdot 17$ fails since 594 is not divisible by $4 = 5 - 1$.

$715 = 5 \cdot 11 \cdot 13$ fails since 714 is not divisible by $4 = 5 - 1$.

$935 = 5 \cdot 11 \cdot 17$ fails since 934 is not divisible by $4 = 5 - 1$.

$1105 = 5 \cdot 13 \cdot 17$ is another Carmichael number since 1104 is divisible by $4, 12$ and 16.

To check that this is the next Carmichael number using just what we've seen so far, you need to check that none of $3 \cdot 5 \cdot p$ (for p a prime up to 73), $3 \cdot 7 \cdot p$ (for p a prime up to 47), etc are Carmichael numbers. This is tedious but doable. You can also use modular arithmetic to reduce the amount of work. Whatever approach you choose, it turns out that $\boxed{1105}$ is in fact the next Carmichael number.

2. **In this problem, we explore a way to defeat Carmichael numbers: the Miller-Rabin primality test.**

   (a) **We've seen that 5 is not a Fermat witness for 561, because 561 is a Carmichael number. So $5^{560} \equiv 1 \pmod{561}$, but we can consider smaller powers of 5. In particular, we factor $560 = 2^4 \cdot 35$.**
   Compute 5^{35}, then $5^{70}, 5^{140}, 5^{280}$, and $5^{560} \pmod{561}$
   We have

$$\begin{aligned} 5^2 &\equiv 25 \\ 5^4 &\equiv 64 \\ 5^8 &\equiv 169 \\ 5^{16} &\equiv -60 \\ 5^{32} &\equiv 256 \\ 5^{35} &\equiv 256 \cdot 25 \cdot 5 \\ &\equiv \boxed{23} \\ 5^{70} &\equiv \boxed{-32} \\ 5^{140} &\equiv \boxed{-98} \\ 5^{280} &\equiv \boxed{67} \\ 5^{560} &\equiv \boxed{1} \pmod{561} \end{aligned}$$

   (b) **Find the last one in this sequence that is not 1. If 561 were prime, there would be only two numbers that squared to 1: 1 and -1. Why is this?**
   Suppose that some other a satisfied $a^2 \equiv 1 \pmod{561}$. Then $a^2 - 1 = (a+1)(a-1) \equiv 0 \pmod{561}$, and must therefore be divisible by 561. If 561 were prime, this would imply that either $a - 1$ or $a + 1$ must be divisible by 561, ie $a \equiv 1 \pmod{561}$ or $a \equiv -1 \pmod{561}$. If we have some other number squaring to 1, then 561 cannot be prime.

   (c) **Can one conclude from this information that 561 is composite? If so, how?**
   See the above explanation for how one can conlcude that 561 must be composite.

(d) **Use this test again with** $3 \pmod{91}$ **to check if** 91 **is composite.**

$$\begin{aligned}
3^2 &\equiv 9 \\
3^4 &\equiv -10 \\
3^8 &\equiv 9 \\
3^{16} &\equiv -10 \\
3^{32} &\equiv 9 \\
3^{45} &\equiv 3^{32} \cdot 3^8 \cdot 3^4 \cdot 3 \\
&\equiv 9 \cdot 9 \cdot -10 \cdot 3 \\
&\equiv 27 \\
3^{90} &\equiv 1 \pmod{91}
\end{aligned}$$

Since $27^2 \equiv 1 \pmod{91}$, 91 is not prime.