Computational Number Theory - Final Exam

Philip Warton

March 15, 2021

Problem 1

Compute 3^{267} mod 100. We can factor 267 as follows,

$$267 = 256 + 8 + 2 + 1$$

Then we can take powers of 3 by squaring,

$$\begin{aligned}
3^1 &\equiv 3 \mod 100 \\
3^2 &\equiv 9 \\
3^4 &\equiv 81 \\
3^8 &\equiv 81^2 \equiv 61 \\
3^{16} &\equiv 61^2 \equiv 21 \\
3^{32} &\equiv 21^2 \equiv 41 \\
3^{64} &\equiv 41^2 \equiv 81 \\
3^{128} &\equiv 81^2 \equiv 61 \\
3^{256} &\equiv 21
\end{aligned}$$

Then write our exponent as a product of these,

$$\begin{aligned}
3^{267} &= 3^{256+8+2+1} \mod 100 \\
&= 3^{256} 3^8 3^2 3^1 \\
&\equiv (21)(61)(9)(3) \\
&\equiv (81)(9)(3) \\
&\equiv (29)(3) \\
&\equiv 87 \mod 100
\end{aligned}$$

Problem 2

We want to factor 731 using Fermat factorization. We know ceil$(\sqrt{731}) = 28$. Then we know $28^2 = 224 + 560 = 784$. We write

$$\begin{aligned}
28^2 - 731 &= 784 - 731 = 53 \\
29^2 - 731 &= 841 - 731 = 110 \\
30^2 - 731 &= 900 - 731 = 169 = 13^2
\end{aligned}$$

So then we say that $731 = (30 - 13)(30 + 13) = (17)(43)$.

Problem 3

We say that $x^2 \equiv 15 \mod 211$ has no solutions by its Legendre symbol. Notice that $211 = 208 + 3 \equiv 3 \mod 4$. So we write,

$$\begin{aligned}\left(\frac{15}{211}\right) &= \left(\frac{3}{211}\right)\left(\frac{5}{211}\right) \\ &= (-1)\left(\frac{211}{3}\right)\left(\frac{211}{5}\right) && \text{(quadratic reciprocity)} \\ &= (-1)\left(\frac{1}{3}\right)\left(\frac{1}{5}\right) \\ &= -1\end{aligned}$$

Problem 4

Proof. We show that $21|n^7 - n$ for every $n \in \mathbb{N}$. First we will show that the quantity is divisble by 3, and then by 7, which will of course imply that it is divisible by 21. First we rewrite

$$n^7 - n = n(n^6 - 1) = n(n^3 + 1)(n^3 - 1)$$

So then if 3 divides any one of those multiplied terms it is granted that $3|n^7 - n$. If $n \equiv 0$ mod 3 then of course the n term is divisble by 3. If $n \equiv 1$ mod 3 then we say $n = 3k + 1$ and

$$n^3 - 1 = (3k + 1)^3 - 1 = (3k)p(k) + 1 - 1 = (3)(k)p(k)$$

Where $p(k)$ is some polynomial of k. We know that the only term without a $(3k)$ factor is the $1^3 = 1$ term i.e. the scalar term cubed (by distributivity of multiplication one could show this rigorously), giving us this result. So in this case $3|n^3 - 1$. Now if $3 \equiv 2$ mod 3, we have

$$n^3 + 1 = (3k + 2)^3 + 1 = (3k)p(k) + 2^3 + 1 = (3)kp(k) + 9 = (3)(kp(k) + 3)$$

So we say that $3|n^3 + 1$. So for all possible n modulo 3, we have either $3|n,\ 3|n^3 + 1$, or $3|n^3 - 1$.

Now we wish to show that $7|(n)(n^3 + 1)(n^3 - 1)$ for every $n \in \mathbb{N}$. If $n = 7k$, clearly $7|n$. Then if $n = 7k + 1$, we have

$$(7k + 1)^3 - 1 = (7k)(p(k)) + 1 - 1 = (7)(kp(k))$$

Then if $n = 7k + 2$,

$$(7k + 2)^3 - 1 = (7k)(p(k)) + 2^3 - 1 = (7k)(p(k)) + 7$$

Following this argument, we can simply check that each number $0, 1, 2, 3, \cdots, 6$ cubed is equal to ± 1 mod 7, to see if 7 divides $(n^3 + 1)(n^3 - 1)$.

$$\begin{aligned}3^3 &= 27 \equiv -1 \mod 7 \\ 4^3 &= 64 \equiv 1 \mod 7 \\ 5^3 &= 125 \equiv -1 \mod 7 \\ 6^3 &= 216 \equiv -1 \mod 7\end{aligned}$$

So for any $7k + r, 0 \leqslant r \leqslant 6$, that is for any n, we have $7|(n)(n^3 + 1)(n^3 - 1)$. So then it follows that $21|n^7 - n$. $\square$

Problem 5

Proof. We want to show that $q|2^p - 1$ where p is a prime equivalent to 3 mod 4. and $q = 2p + 1$. We write $p = 4k + 3$ and then $q = 2(4k + 3) = 8k + 7$. So then it follows that

$$\left(\frac{2}{q}\right) = 1$$

That is, $\exists x$ such that $x^2 \equiv 1 \bmod q$. Now, by Fermat's Little Theorem we have

$$\begin{aligned}
x^{q-1} &\equiv 1 \mod q \\
x^{2(q-1)/2} &\equiv 1 \quad \vdots \\
x^{2p} &\equiv 1 \\
(x^2)^p &\equiv 1 \\
2^p &\equiv 1 \\
2^p - 1 &\equiv 0 \mod q
\end{aligned}$$

The final statement is equivalent to $q|2^p - 1$. $\square$