

book problems

§8.1 # 4. Let r be the order of $ab \pmod{n}$. By Thm 8.1 to show $r \mid hk$ it is enough to show that $(ab)^{hk} \equiv 1 \pmod{n}$. But this is clear since $(ab)^{hk} = (a^h)^k (b^k)^h \equiv 1 \pmod{n}$. To see that if $\gcd(h, k) = 1$ then $r = hk$ it is enough to show that $h \mid r$ and $k \mid r$. To see this consider the order of $(ab)^h$. On the one hand this is $\frac{r}{\gcd(r, h)}$. But on the other hand, $(ab)^h$ is just b^h which has order $\frac{k}{\gcd(k, h)} = k$. Therefore we see $\frac{r}{\gcd(r, h)} = k$ or put another way, $r = k \gcd(r, h)$. Thus, $k \mid r$. A similar argument shows that $h \mid r$.

Non-book problems:

Using the function `isprime` in GP/PARI we quickly see that 9999991 is a prime number. Therefore by what we have seen in class, 9999991 has a primitive root of unity. Using the function `znprimroot` in GP/PARI we quickly find out that 22 is a primitive root of 9999991. Therefore, all other numbers $1 \leq k \leq 9999990$ are equal mod 9999991 to 22^h for some $1 \leq h \leq 9999990$. Now by our theorem in class the order of 22^h is $9999990 / \gcd(h, 9999990)$. So to get order 2,3,4 or 5, we know what h should be.

- a). There are 3 solutions to this equation. $x = 1, 22^{3333330}, 22^{6666660}$ are solutions to $x^3 \equiv 1 \pmod{9999991}$. The least non-negative residues of these numbers are $x = 1, 9972972$, and 27018
- b). There are two solutions to the equation $x^4 \equiv 1 \pmod{9999991}$. They are $x = 1$ and $x \equiv 22^{4999995} \pmod{9999991}$. The reduced residues are $x = 1, 9999990$.
- c). There are 5 solutions to this equation. Let

$$k = 0, 1999998, 3999996, 5999994, 7999992.$$

Then the solutions to $x^5 \equiv 1 \pmod{9999991}$ are of the form $22^k \pmod{9999991}$. The reduced residues are the numbers $x = 1, 1695067, 4720414, 5199016$, and 8385484 .