Math 365 - Quiz 4

Name and Student ID:

Question: a) Show that $r = 5$ is a primitive root of $p = 23$.
b) Solve the congruence $x^3 \equiv 20 \pmod{23}$.
c) Is 20 a quadratic residue of 23?

a) r is a primitive root of p iff order of r is $\varphi(p) = \varphi(23) = 23 - 1 = 22$
Let k be order of $r = 5$ modulo 23.
Then $k \mid \varphi(23)$, so $k \mid 22 \Rightarrow k \in \{1, 2, 11, 22\}$

$r^1 \equiv 5 \not\equiv 1 \pmod{23}$, $r^2 \equiv 25 \equiv 2 \not\equiv 1 \pmod{23}$
(so $k \neq 1$) (so $k \neq 2$)

$r^4 \equiv 2 \cdot 2 \equiv 4 \pmod{23}$, $r^8 \equiv 4^2 \equiv 16 \pmod{23}$

$r^{11} \equiv r^8 \cdot r^2 \cdot r^1 \equiv 16 \cdot 2 \cdot 5 \equiv 160 \equiv 22 \equiv -1 \not\equiv 1 \pmod{23}$
(so $k \neq 11$)

$k \neq 1, k \neq 2$ and $k \neq 11 \Rightarrow k = 22$.
Therefore $r = 5$ is a primitive root of 23.

b) Let's use $r = 5$ as a primitive root. To find the index of 20 relative to $r = 5$,

$5^1 \equiv 5 \pmod{23}$, $5^2 \equiv 2 \pmod{23}$ $5^3 \equiv 10 \pmod{23}$ $5^4 \equiv 50 \equiv 4 \pmod{23}$

$5^5 \equiv 4 \cdot 5 \equiv 20 \pmod{23} \Rightarrow \text{ind}_5 20 = 5$ modulo 23.

Let $x \equiv 5^y \pmod{23}$ where $y = \text{ind}_5 x$.

$x^3 \equiv 20 \pmod{23} \Leftrightarrow (5^y)^3 \equiv 5^5 \pmod{23}$

$\Leftrightarrow 5^{3y} \equiv 5^5 \pmod{23}$

$\Leftrightarrow 3y \equiv 5 \pmod{\varphi(23)}$

$3y \equiv 5 \pmod{22}$

$15 \cdot 3y \equiv 15 \cdot 5 \pmod{22}$

$45y \equiv 75 \pmod{22}$

$y \equiv 9 \pmod{22}$

Since $\gcd(3, 22) = 1$, there is a unique solution y modulo 22.
Then, $x \equiv 5^y \equiv 5^9 \pmod{23} \Rightarrow x \equiv 5^8 \cdot 5^1 \equiv 16 \cdot 5 \equiv 80 \equiv 11 \pmod{23}$
$x \equiv 11 \pmod{23}$ is the unique solution.

c) $a=20$ is a quadratic residue of 23

$\Leftrightarrow x^2 \equiv 20 \pmod{23}$ has a solution

$\Leftrightarrow (20/23) = 1$ (Legendre Symbol)

$(20,23) = (4\cdot 5/23) = (4/23)\cdot(5/23)$

$= (2^2/23)\cdot(5/23)$

by Quadratic Reciprocity Law $= 1\cdot(-1)^{\frac{5-1}{2}\cdot\frac{23-1}{2}}\cdot(23/5)$

since $23 \equiv 3 \pmod 5$ $\leftarrow$ $= (23/5) = (3/5)$

$= (-1)^{\frac{3-1}{2}\cdot\frac{5-1}{2}}\cdot(5/3)$

$a \equiv b \pmod p$

$\Rightarrow (a/p) = (b/p)$

$= (5/3) = (2,3) = -1$

since $3 \equiv 3 \pmod 8$

by the Thm about

$(2,p) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$