book problems

9.3 #9. Let $p$ and $q$ be odd primes satisfying $p = q + 4a$ for some $a$. Show that $(a/p) = (a/q)$. This follows from the following sequence of equalities.

$$(a/p) = (- (p - 4a)/p) = (- q/p) = (-1)^{p-1/2} (q/p) = (-1)^{p-1/2 + q-1/2} (p/q)$$

$$= (-1)^{p-1/2 (1 + q-1/2)} (4a + q/q) = (-1)^{p-1/2 (1 + q-1/2)} (a/q).$$

Now, since $q \equiv p \pmod{4}$ the numbers $(p - 1)/2$ and $(q - 1)/2$ have the same parity. Thus one of $(p - 1)/2$ or $1 + (q - 1)/2$ are even and as a result $(-1)^{p-1/2 (1 + q-1/2)} = 1$. We are done.

Non-book problems: 1. Let $r$ be a primitive root of $p$. $r$ has order $p - 1 = 3k + 1$. Now, the order of $r^3$ is $\frac{3k + 1}{\gcd(3k + 1, 3)} = 3k + 1 = p - 1$. That is, $r^3$ also has order $p - 1$. Therefore, the least non-negative residues of $r^3, (r^3)^2, \ldots, (r^3)^{p-1}$ run through $1, 2, \ldots, p - 1$. That is, every least non-negative residue is a cubic residue.

2. Again, let $r$ be a primitive root of $p$, having order $3k$. This time, the order of $r^3$ is $\frac{3k}{\gcd(3k, 3)} = k$. Therefore, the integers $r^3, (r^3)^2, \ldots, (r^3)^k$ are incongruent mod $p$ and are cubic residues. These are one third of the (non-zero) residues. Now, if $y$ is a cubic residue, then $y = x^3$ for some $x = r^j$ for some $j$. Then $y = (r^j)^3 = (r^3)^j$. Let $j' < k$ be congruent to $j$ mod $k$, then $y \equiv (r^3)^{j'} \pmod{p}$ and hence is one of the elements already listed.