AC, 7^{th} December 2006

M3P14 Elementary Number Theory
Assessed Coursework 3: Solutions.

(2) From the way we did things in class, it is natural to take these assertions in the order (i), (iii), (iv), (ii); I am sorry if this has caused you some difficulty.
(i) We want to show that

$$\frac{n^2-1}{8} \quad \text{is} \quad \begin{cases} \text{even if} & n \equiv 1,7 \mod 8 \\ \text{odd if} & n \equiv 3,5 \mod 8 \end{cases}$$

There are four small calculations to do. For example, if $n = 8k+1$, then

$$n^2 = 64k^2 + 16k + 1$$

and $\frac{n^2-1}{8} = 2k(4k+1)$ is even. Similarly, if $n = 8k+3$, then

$$n^2 = 64k^2 + 48k + 9$$

and $\frac{n^2-1}{8} = 2k(4k+3)+1$ is odd. The cases $n = 8k+5$ and $n = 8k+7$ are similar.
(iii) Let us write $a = 2k+1$ and $b = 2h+1$. Then

$$a^2b^2 - a^2 - b^2 - 1 = (a^2-1)(b^2-1) = 16kh(k-1)(h-1)$$

is divisible by 16, therefore

$$\frac{a^2b^2 - a^2 - b^2 - 1}{8} = \frac{a^2b^2-1}{8} - \frac{a^2-1}{8} - \frac{b^2-1}{8} \equiv 0 \mod 2.$$

(iv) Follows almost immediately from (iii).
(ii) We know that if p is an odd prime then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if} \quad p \equiv 1,7 \mod 8 \\ -1 & \text{if} \quad p \equiv 3,5 \mod 8 \end{cases}$$

By what we did in part (i) then

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} \tag{1}$$

if p is prime. The result follows for all n by factorizing n into primes, because boths sides of Equation 1 are multiplicative in n.

(3) Here we go:

$$\begin{aligned}
\left(\frac{5}{13}\right) &= \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{2}{3}\right) = -1; \\
\left(\frac{13}{13}\right) &= 0; \\
\left(\frac{456}{123}\right) &= \left(\frac{-36}{123}\right) = \left(\frac{-1}{123}\right)\left(\frac{6}{123}\right)^2 = \left(\frac{-1}{123}\right)0^2 = 0; \\
\left(\frac{11}{10001}\right) &= \left(\frac{10001}{11}\right) = \left(\frac{2}{11}\right) = -1.
\end{aligned}$$

(8) (i) This always happense if $\mathrm{hcf}(a, n) = 1$ and a is a square mod n. Indeed then a is a square mod p for every prime p that divides n, so $\left(\frac{a}{p}\right) = 1$ for every prime that divides n, and then $\left(\frac{a}{n}\right) = 1$ by definition of the Jacobi symbol.
(ii) This can happen if $\mathrm{hcf}(a, n) \neq 1$; for example if $n = p$ is prime, and $p|a$, then by definition $\left(\frac{a}{p}\right) = 0$ but $a \equiv 0 \mod p$ is certainly a square mod p.
(iii) This can happen and we saw an example in class; take $n = 15$ and $a = -1$; then $\left(\frac{-1}{15}\right) = 1$ but -1 is not a square mod 15.
(iv) This can also happen; for example every time that $n = p$ is prime and $p \not| a$.

(10) This is fun: first, we look at

$$y^2 = x^3 + 23$$

modulo 4; $y^2 \equiv 0$ or 1 mod 4; correspondingly, $x^3 \equiv 1$ or 2 mod 4; but only the first case is possible with $x \equiv 1$ mod 4 and y even.

Now we have

$$y^2 + 4 = x^3 + 27 = (x + 3)(x^2 - 3x + 9)$$

and the factor $x^2 - 3x + 9 \equiv 3 \mod 4$, so it is the product of odd primes and at least one of them, say $p \equiv 3$ mod 4. From

$$y^2 + 4 \equiv 0 \mod p$$

we get $\left(\frac{-1}{p}\right) = 1$, a contradiction.