The purpose of this note is to provide a proof that in the signature verification we have \( v = r \) if the signature is valid. The following proof is based on that which appears in the FIPS standard, but it includes additional details to make the derivation clearer.

**LEMMA 1.** For any integer \( t \), if \( g = h^{(p-1)/q} \mod p \)

\[
g^t \mod p = g^{t \mod q} \mod p
\]

**Proof:** By Fermat's theorem (Chapter 8), because \( h \) is relatively prime to \( p \), we have

\[ H^{p-1} \mod p = 1. \]

Hence, for any nonnegative integer \( n \),

\[
g^{nq} \mod p = h^{(p-1)/q} \mod p^{nq} \mod p
\]

\[
= h^{(p-1)/q} \mod p \quad \text{by the rules of modular arithmetic}
\]

\[
= h^{(p-1)n} \mod p
\]

\[
= h^{(p-1)} \mod p \quad \text{by the rules of modular arithmetic}
\]

\[
= 1^n \mod p = 1
\]

So, for nonnegative integers \( n \) and \( z \), we have

\[
g^{nq+z} \mod p = (g^{nq} g^z) \mod p
\]

\[
= \left( (g^{nq} \mod p)(g^z \mod p) \right) \mod p
\]

\[
= g^z \mod p
\]
Any nonnegative integer \( t \) can be represented uniquely as \( t = nz \), where \( n \) and \( z \) are nonnegative integers and \( 0 < z < q \). So \( z = t \mod q \). The result follows. QED.

**Lemma 2.** For nonnegative integers \( a \) and \( b \):
\[
g^{(a \mod q + b \mod q)} \mod p = g^{(a+b) \mod q} \mod p
\]

**Proof:** By Lemma 1, we have
\[
g^{(a \mod q + b \mod q)} \mod p = g^{(a \mod q + b \mod q)} \mod q \mod p
\]
\[
= g^{(a+b) \mod q} \mod p
\]
QED.

**Lemma 3.**
\[
y^{(rw) \mod q} \mod p = g^{(xrw) \mod q} \mod p
\]

**Proof:** By definition (Figure 13.2), \( y = g^x \mod p \). Then:
\[
y^{(rw) \mod q} \mod p = (g^x \mod p)^{(rw) \mod q} \mod p
\]
\[
= g^x ((rw) \mod q) \mod p
\]
by the rules of modular arithmetic
\[
= g^{x ((rw) \mod q)} \mod q \mod p
\]
by Lemma 1
\[
= g^{(xrw) \mod q} \mod p
\]
QED.

**Lemma 4.**
\[
((H(M) + xr)w) \mod q = k
\]
**Proof:** By definition (Figure 13.2), \( s = \left( k^\Pi \left( H(M) + xr \right) \right) \mod q \). Also, because \( q \) is prime, any nonnegative integer less than \( q \) has a multiplicative inverse (Chapter 8). So \((k \cdot k^{-1}) \mod q = 1\).

Then:

\[
(ks) \mod q = \left[ k \left( k^\Pi \left( H(M) + xr \right) \right) \mod q \right] \mod q
\]

\[
= \left[ k \left( k^\Pi \left( H(M) + xr \right) \right) \mod q \right] \mod q
\]

\[
= \left( (kk^\Pi) \mod q \right) \left( (H(M) + xr) \mod q \right) \mod q
\]

\[
= \left( (H(M) + xr) \right) \mod q
\]

By definition, \( w = s^{-1} \mod q \) and therefore \((ws) \mod q = 1\). Therefore,

\[
((H(M) + xr)w) \mod q = (((H(M) + xr) \mod q) (w \mod q)) \mod q
\]

\[
= ((ks) \mod q) (w \mod q)) \mod q
\]

\[
= (kws) \mod q
\]

\[
= ((k \mod q) ((ws) \mod q)) \mod q
\]

\[
= k \mod q
\]

Because \( 0 < k < q \), we have \( k \mod q = k \). **QED.**

**THEOREM:** Using the definitions of Figure 13.2, \( v = r \).

\[
v = \left( g^{u1}y^{u2} \mod p \right) \mod q
\]

\[
= \left( H(M)w \mod q \right) \left( yr \mod q \right) \mod p \mod q
\]
\[
\begin{align*}
&= g^{(H(M)w \mod q)(xrw \mod q) \mod p \mod q} \\
&= g^{(H(M)w) \mod q + (xrw) \mod q \mod p \mod q} \\
&= g^{(H(M)w + xrw) \mod q \mod p \mod q} \\
&= g^{(H(M) + xr)w \mod q \mod p \mod q} \\
&= (gk \mod p) \mod q \quad \text{by Lemma 4} \\
&= r \quad \text{by definition}
\end{align*}
\]

QED.